NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

A SECURITY RISK MEASUREMENT FOR THE RADAC MODEL

by

David W. Britton
Ian A. Brown

March 2007

Thesis Advisor:	George Dinolt
Second Reader:	Karl Pfeiffer

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** March 2007	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE A Security Risk Measurement for the RAdAC Model	**5. FUNDING NUMBERS**
6. AUTHOR(S) David Britton and Ian Brown	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

The purpose of this thesis is to provide a quantification process for the risk module of the NSA RAdAC model. The intent is to quantify the risk involved in a single information transaction. Additionally, this thesis will attempt to identify the risk factors involved when calculating the total security risk measurement. This list is not intended to be an all-inclusive list of every factor associated with a transaction. Rather, we intend to supply a pragmatic list that is easily scalable to specific situations to include those factors which have the greatest effect on the total security risk measurement. In addition, we have asked experts in multiple fields to provide us with their opinion on the weighting of the risk factors. Finally, these weight sets and concomitant risk factors will be tested for accuracy in an Excel model.

14. SUBJECT TERMS RAdAC, NSA, risk factors, security risk, quantification process, information transaction	**15. NUMBER OF PAGES** 89
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

THIS PAGE INTENTIONALLY LEFT BLANK

A SECURITY RISK MEASUREMENT FOR THE RADAC MODEL

David W. Britton
Lieutenant, United States Navy
B.A., Virginia Tech, 1999

Ian A. Brown
Lieutenant, United States Navy
B.S., Norfolk State University, 2001

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
March 2007

Authors: David W. Britton
Ian A. Brown

Approved by: George Dinolt
Thesis Advisor

Karl Pfeiffer
Second Reader

Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The purpose of this thesis is to provide a quantification process for the risk module of the NSA RAdAC model. The intent is to quantify the risk involved in a single information transaction. Additionally, this thesis will attempt to identify the risk factors involved when calculating the total security risk measurement. This list is not intended to be an all-inclusive list of every factor associated with a transaction. Rather, we intend to supply a pragmatic list that is easily scalable to specific situations to include those factors which have the greatest effect on the total security risk measurement. In addition, we have asked experts in multiple fields to provide us with their opinion on the weighting of the risk factors. Finally, these weight sets and concomitant risk factors will be tested for accuracy in an Excel model.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We would like to thank Dr. George Dinolt and Lt Col Karl Pfeiffer for providing us with guidance and direction in the development of our thesis. Their constant encouragement and insightful discussions were invaluable as our research progressed.

We would also like thank our wives and children for supporting us throughout this challenging process. Our families are what kept us going when we spent too much time in front of a computer or too many hours reading through books.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. BACKGROUND

Risk Adaptable Access Control (RAdAC) as formulated by the National Security Agency (NSA) is the concept for the next generation access control method based on a predetermined set of conventional and digital policies (McGraw, 2006). Digital policies are defined such that they can be understood and evaluated by computers, vice conventional policies that are in the form of paper documents (Choudhary, 2005). In tomorrow's war-fighting environment, a commander must be allowed the leeway to make exceptions to rules when the operational need for information outweighs the risk of sharing it and do it having all of the information required to make a sound decision. The implementation of the RAdAC engine will significantly enhance a commander's overall situational awareness by automatically and instantaneously measuring the total security risk and operational need of the information transaction and then weighing those measurements against the conventional and digital policies previously established.

The current method for sharing information is based on a combination of both MAC and DAC (McGraw, 2006). An individual's clearance level must match or exceed the classification level of the information requested. In addition, the other stipulation inherent to accessing any information is the individual's "need to know." The combination of these methods of sharing information lack the flexibility required to support the objectives for the information superiority vision of the GIG (Net-Centric Operational Environment Joint Integrating Concept, 2005).

In the future, a "need to share" philosophy will allow information access to those who need it, when they need it. The recent 9/11 and Hurricane Katrina disasters have demonstrated the obligation to prevent the stove-piping of information. As technology rapidly evolves, the mandate to be able to securely share information rapidly and dynamically is paramount. RAdAC is the access control method that will account for the total security risk and operational need of an information transaction and will allow that "need to share" philosophy to succeed.

B. THESIS OVERVIEW

The purpose of this thesis is to provide a quantification process for the risk module of the NSA RAdAC model. The intent is to quantify risk involved in a single information transaction. The first step in this thesis will identify the risk factors involved when calculating the total security risk measurement. Using the NSA identified risk categories we will create a list of possible factors that can be used in a RAdAC engine. This list is not intended to be an all-inclusive list of every factor associated with a transaction. An in-depth analysis of individual transactions is not only impractical from a time standpoint, but it would also be extremely complex and cumbersome. Rather, we intend to supply a pragmatic list that is easily scalable to specific situations to include those factors which have the greatest effect on the total security risk measurement.

Next we will create a quantification process to calculate a Total Security Risk Measurement. The process will assign a value to each of the individual factors and then be run through a model to create the final risk value. A weighting scheme for the risk factors will be developed to be used in the model and finally, this list and concomitant risk factors will be tested for accuracy and practicality through the use of boundary case scenarios.

C. CHAPTER OVERVIEW

The first chapter will cover the scope of our thesis to include a description of items that we will include in the thesis as well as a list of assumptions. Next, the problem proposal and methodology will be briefly explained and will contain a description of our implementation and testing methods. The final subsection of Chapter I will examine the expected benefits of our research.

D. SCOPE

This thesis will identify a set of risk factors associated with an information transaction in the NSA RAdAC model. We will not attempt to identify the interdependency of the factors or find any correlating factors. The second component to this thesis will be the identification of a process to quantitatively measure risk including a measure of uncertainty. The focus will be on the security risk measurement in the Policy Decision Point and will not cover any portion of the operational need measurement or the policies that calculate the final policy decision.

E. ASSUMPTIONS

The transaction initiator (human or machine) is who he says he is. The authentication problem will not be accounted for in this thesis. This includes all components of the system used for initiation and transmission of the transaction.

There are no hardware/software failures. We will not account for uncertainty associated with human or machine error. In addition, all components work as they are intended to work.

The information is available and accurate. This model does not account for risk involved with information integrity or availability. This process will also not address the issue of the information being compromised during transmission.

The factors identified are independent for the purposes of the risk measurement process. We do not account for any interdependencies.

F. PROBLEM PROPOSAL AND METHODOLOGY

This thesis will focus on developing a general transactional risk model that can be integrated into the RAdAC Policy Decision Point. We will first identify a set of risk factors that correspond to the RAdAC risk categories. The risk categories include factors that relate to the individuals involved, data requested, IT components, situational factors, environmental factors, and heuristics surrounding the transaction. Without historical data to determine an actual statistical distribution, we will use Excel to create a triangle distribution to calculate the risk of each factor. The triangle distribution calculates the amount of risk using a minimum, maximum and most likely value assigned by the user (Mun, 2004). We will then use Monte Carlo simulation to add uncertainty to the risk factor measurement. The model will then calculate a total security risk based on the most likely inputs from the triangle distribution multiplied by a set of weighting factors. The weighting factors will be derived from interviewing experts in the fields of business, computer science, physical security and information assurance. Finally we will test the model for accuracy using several boundary case scenarios.

G. EXPECTED BENEFITS OF RESEARCH

This thesis will identify many of the risk factors associated with RAdAC. It will also identify a process to quantify the risk factors that can be used to build a Digital Risk

Policy. Other benefits of the research will be included in a section on paths taken that ended with dead-ends and further questions that need to be answered before RAdAC can be implemented.

II. RADAC

A. CHAPTER OVERVIEW

There already are many DoD requirements that will depend on RAdAC to function properly. This chapter will briefly discuss those documents that have stated a requirement for a working RAdAC engine including the Global Information Grid (GIG), NetOps, and the Net-Centric Operational Environment (NCOE). In addition, this chapter will include background on the current access control methods of Mandatory Access Control (MAC), Discretionary Access Control (DAC), Role Based Access Control (RBAC) and an overview of Multilevel Security (MLS). Finally, Chapter II will provide an in-depth look at the NSA RAdAC model. It will cover the policy architecture followed by a description of the individual modules that comprise the whole, as well as a discussion of the policies themselves and the management of the conventional and digital policies that drive the concept.

B. DOD TRANSFORMATION GUIDANCE

1. Global Information Grid

> As we prepare for the future, we must think differently and develop the kinds of forces and capabilities that can adapt quickly to new challenges and to unexpected circumstances. We must transform not only the capabilities at our disposal, but also the way we think, the way we train, the way we exercise and the way we fight. We must transform not only our armed forces, but also the Department that serves them by encouraging a culture of creativity and prudent risk-taking.
>
> Donald Rumsfeld (Transformation Planning Guidance, 2003)

The Department of Defense (DoD) Transformation Planning Guidance (2003) defines the desired outcome of transformation as “fundamentally joint, network-centric, distributed forces capable of rapid decision superiority and massed effects across the battle space.” The Defense Acquisition Guidebook (2006) defines Net-centricity as

> The realization of a robust, globally networked environment within which data is shared seamlessly and in a timely manner among users, applications, and platforms. By securely interconnecting people and systems, independent of time or location, net-centricity enables substantially improved military situational awareness and significantly shortened decision making cycles. Users are empowered to better protect

> assets; more effectively exploit information; more efficiently use resources; and unify our forces by supporting extended, collaborative communities to focus on the mission.

The DoD's approach for transforming to net-centric operations and warfare uses the GIG as "the organizing and transforming construct for managing information technology throughout the Department" (Defense Acquisition Guidebook, 2006). The GIG and its assets are defined in DoD Directive 8100.1 (2002) as follows

> The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data security services, and other associated services necessary to achieve Information Superiority. The GIG supports all DoD, National Security, and related Intelligence Community missions and functions (strategic, operational, tactical, and business) in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites) and provides interfaces to coalition, allied and non-DoD users and systems.

The vision of the GIG is to empower users through easy access to information anytime, anyplace, under any conditions with attendant security to achieve Information Superiority as shown in Figure 1.

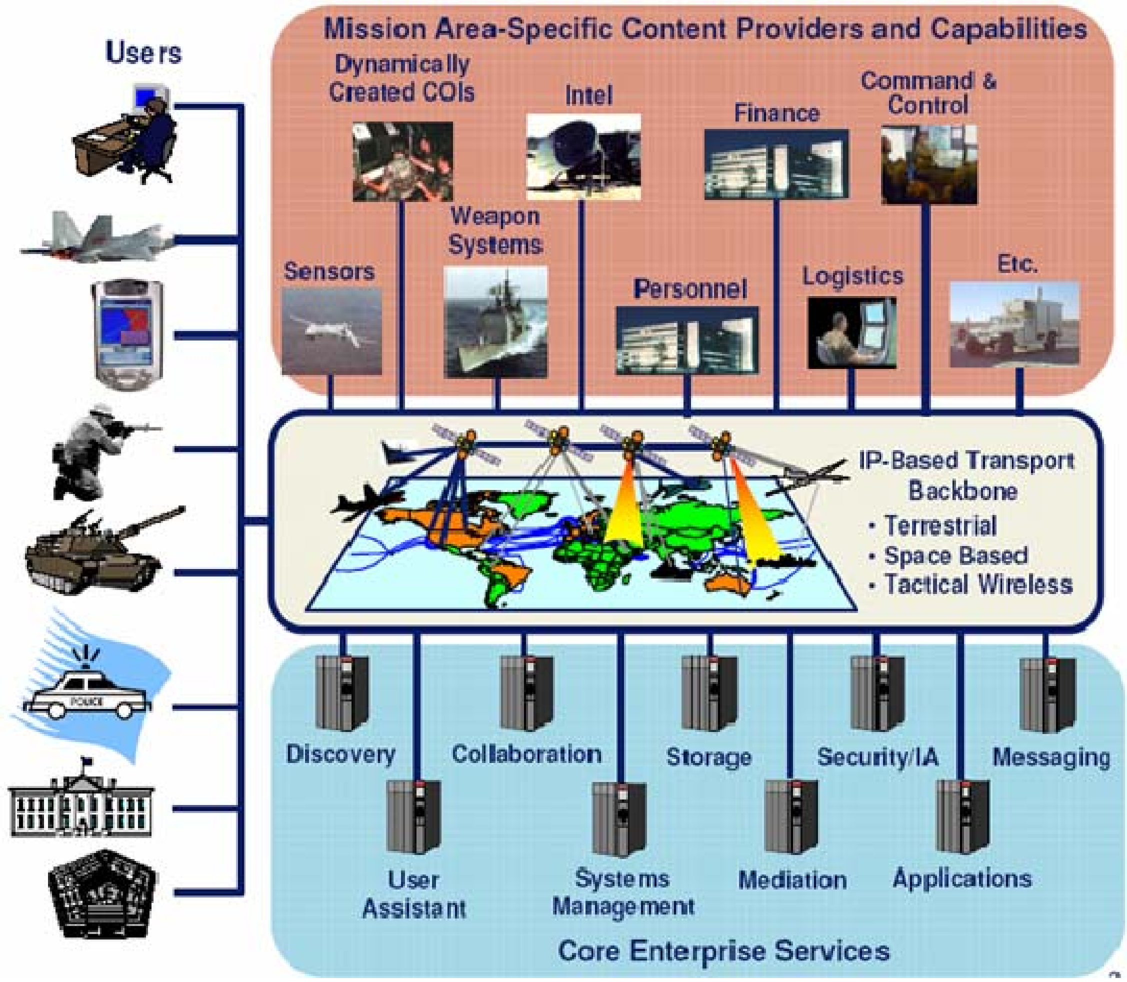


Figure 1. GIG Vision (From: McGraw, 2004)

2. NetOps

Commander, US Strategic Command (CDRUSSTRATCOM) is assigned the responsibility to operate and defend the GIG. NetOps is the operational tool that CDRUSSTRATCOM will use to achieve that mission. NetOps, as stated in the Joint Concept of Operations for Global Information Grid NetOps (2005), consists of three primary functions: Essential tasks, Command and Control (C2), and Situational Awareness (SA). Each of the definitions from the NetOps document is provided below.

a. Essential Tasks

NetOps uses an integrated approach to accomplish the three interdependent essential tasks necessary to operate and defend the GIG. These tasks are GIG Enterprise Management (GEM), GIG Network Defense (GND) and Information Dissemination Management / Content Staging (IDM/CS). NetOps is not simply GEM and GND and IDM/CS tacked together. Rather, it is the methodical integration of individual capabilities and the resultant synergy.

b. Command and Control

NetOps C2 will provide a seamless C2 environment that is dynamic, decentralized, distributed, and enabled by robust, secure and integrated networks. NetOps C2 will be able to create desired GIG effects at the right time and place to accomplish the mission.

c. Situational Awareness

NetOps will provide a shared SA to improve the quality and timeliness of collaborative decision-making regarding the employment, protection and defense of the GIG. Much of this GIG SA will be available and shared in near real-time by the relevant decision-makers.

3. Net-Centric Operational Environment

The Net-Centric Operational Environment (NCOE) is an operational subset of the GIG (Net-Centric Operational Environment Joint Integrating Concept, 2005). The NCOE uses the NetOps framework but also expands it by incorporating knowledge management (KM), network management (NM), and information assurance (IA). The NCOE is supported by its Enabling Constructs which includes a comprehensive matrix of Capabilities, Tasks and Standards. Section 7.11 of this matrix lists RAdAC as a technical capability needed for the NCOE to achieve the ability to identify, store, share, and exchange data and information.

C. CURRENT ACCESS CONTROL METHODS

Access controls are security features that control how users and systems communicate and interact with other systems and resources (Harris, 2003). They are used to permit or deny the use of an object, such as a system or file, by a subject such as an individual or process. Access control mechanisms are a necessary and crucial design element of any application’s security. Ideally, an access control mechanism should protect against the unauthorized viewing, modification, or copying of data. Additionally, access control mechanisms should limit malicious code execution and unauthorized actions through an attacker exploiting infrastructure dependencies.

Access control systems provide the essential services of identification, authentication, authorization, and accountability. Identification and authentication (I&A) determine who can log on to a system. Authorization determines what an authenticated user can do and accountability identifies what a user did (CNSS Instruction No. 4009 National Information Assurance Glossary, 2006). There are several access control systems in the information security realm. A successful access control protection system will likely combine aspects of each of the following mechanisms.

1. Mandatory Access Control

Mandatory access control (MAC) is an access control policy determined by the system, not the data owner. Access decisions are made beyond the control of the individual owner of an object (Pfleeger, 2003). The most important feature of MAC involves denying users full control over the access to resources that they create. The system security policy entirely determines the access rights granted. A user may not grant less restrictive access to their resources than the administrator specifies.

MAC must be non-bypassable, evaluatable, always-invoked and tamper-proof. Controlling the import of information to and export from a system is a critical function of MAC so that sensitive information is appropriately protected at all times.

MAC prevents an authenticated user or process at a specific classification or trust-level from accessing information, processes, or devices at a different level. This provides a mechanism for the containment of users and processes, both known and unknown. In a MAC-based system, all subjects and objects must have security labels assigned to them. A user’s security label, the user’s clearance, specifies their level of trust. An object’s security label, its classification, specifies the level of trust required for access. In order to read a given object, the subject must have a security label equal to or higher than the requested object. In order to write to the object, the subject must have the same classification as the object. MAC mechanisms ensure that all users only have access to that data for which they have clearance and do not write data to objects at lower levels.

2. Discretionary Access Control

Discretionary Access Control (DAC) is a means of restricting access to data based on the identity and need-to-know of users. The controls are discretionary in the sense that the data’s owner determines who should have access rights to the object and what those rights should be (Pfleeger, 2003). The need to know principle is similar to the least privilege principle. It is based on the concept that individuals should only be given access to the information that they absolutely require in order to perform their job duties (Harris, 2003). Normally, the owner of a resource is the person who created the resource. Data owners can determine the level of access given to other users (read, write, copy, etc.) and can transfer ownership of information to other users. A potential security vulnerability of DAC is the ability of data owners, through accident or malice, to give access to unauthorized users.

Access decisions are granted to a user based on the credentials that were presented at the time of authentication. Users who do not have permissions to access the information should also not be able to determine its characteristics such as file size, file name, directory path, etc. Users may belong to one or many groups and can acquire cumulative permissions. They can also be disqualified from any permission that isn't part of every group to which they belong.

3. Role-Based Access Control

Role-Based Access Control (RBAC) is an approach to restricting system access to authorized users based on an individual's role within an organization (Curphey, 2002). RBAC is an alternative approach to MAC and DAC in that it assigns permissions to specific operations with meaning in an organization. RBAC access control systems provide the ability to determine who can perform what actions, when, from where and in what order. Within an organization, roles are created for various job functions and centrally managed by security administrators. Permissions are then assigned to the specific roles based on the principle of least privilege. Users acquire the permissions to perform particular system functions through their role assignments. Since users are not assigned permissions directly, but only acquire them through their roles, management of individual user rights becomes a matter of assigning the appropriate role or multiple simultaneous roles to the user. As complexity of commands or files increases the management and organization of roles becomes more crucial.

4. Multilevel Security

Multilevel Security (MLS) is the capability of a computer system to carry information with different classification levels, permit simultaneous access by users with different security clearances and needs-to-know, and prevent users from obtaining access to information for which they lack authorization (Harris, 2003). MLS systems allow access to less-sensitive information by higher-cleared individuals, and allow them to share sanitized documents with lower-cleared individuals. MLS systems incorporate two essential features. Based on the Bell-LaPadula model or a close variant thereof, the system must enforce access restrictions regardless of the actions of system users or administrators. Second, MLS systems must enforce these restrictions with incredibly high reliability. According to Dr. Rick Smith (2005), "Although Bell-LaPadula has accurately defined a MLS capability that keeps data safe, it has not led to the widespread development of successful multilevel systems." MAC and MLS systems are often, but not always, tied together.

D. RADAC OVERVIEW

1. Basic Architecture

The basic architecture of the NSA RAdAC model has been provided by Dr. Abdur Choudhary (2005) based on the IETF standard policy framework (Yavatkar, Pendarakis, Guerin, 2000). The basic structure starts with an information requestor. This may be a person, system or application. The information transaction request is then routed through the Policy Enforcement Point (PEP). The PEP is responsible for the enforcement of the decision to grant access or deny information from the Policy Decision Point (PDP). The PDP is the "brain" of the RAdAC engine. It consists of the Security Risk Measurement, the Operational Need Measurement and returns the Final Access Decision. Figure 2 shows the high level architecture for the NSA RAdAC model and Figure 3 shows the policy-based architecture.

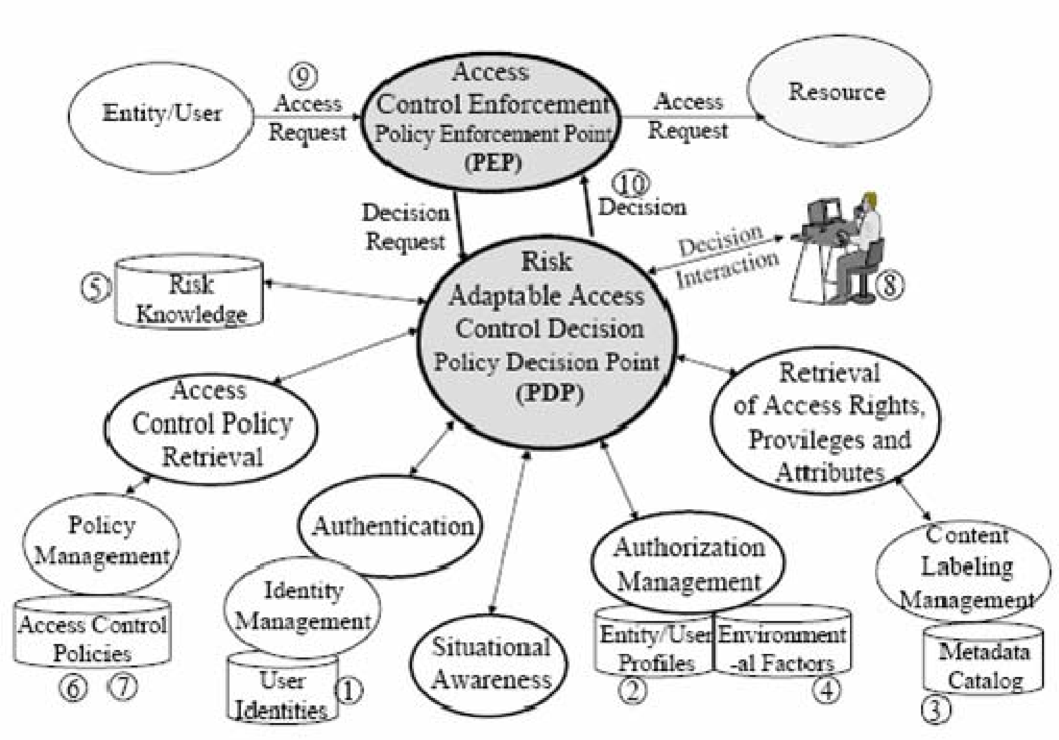


Figure 2. RAdAC High Level Architecture (From: Choudhary, 2005)

2. Policy Management

The dynamic management of the policies is the other lynchpin to making RAdAC successful. The conventional and digital policies must be continually updated for any given situation and commander’s intent. The digital policies, used by both the Security Risk Function and the Operational Need Function, may consist of simple if/then statements. The PBM infrastructure must manage the conventional policies with a minimal set of functions that consist of policy definition, translation, validation, distribution, activation, execution, and audit (Choudhary, 2005).

3. Information Transaction

Rather than clearing an individual access to a certain level of information for what amounts to lifetime trust, RAdAC requires a more granular approach (Horizontal Integration, 2004). Each transaction will be identified, calculated and then reviewed to give the appropriate access. Transaction, in this context, means a single request of classified information (hard or soft copies) for a given amount of time. Examples of an information transaction could include a single classified briefing multicast to involved parties or a hard copy classified document such as an Air Tasking Order given to a pilot or any number of scenarios like these. Allowing a requestor access to multiple information items or levels of information would not allow the RAdAC engine to evaluate the risk or operational need at the appropriate scale.

4. Requestor

The information requestor can be an individual, system or application. The traditional definition for information requestor involves a person with a need for information. RAdAC will stretch the definition to incorporate requestor as machine or application. For example, a weapons system may request positional and weather data for a targeting sequence that may be completely invisible to the trigger puller. In this instance, RAdAC would measure the risk and operational need of a machine to machine transaction.

5. Policy-Based Management

Policy-based management (PBM) is typically used as a way to allocate network resources, primarily network bandwidth, Quality of Service and security, according to pre-defined policies. In the context of RAdAC, PBM can be used to provide real time, dynamic answers about whom and what can access which resources on the network. PBM allows administrators to define rules and manage them in the policy system. These rules take the form "If condition, then action" (Sheldon, 2001). The Internet Engineering Task Force (IETF) Policy Framework Working Group has developed a policy-based management architecture that includes the following components; Policy management service, dedicated policy repository, policy enforcement point, policy decision point, and local policy decision point (Yavatkar, Pendarakis, Guerin, 2000). RAdAC incorporates several of these components into its architecture. Figure 3 shows the RAdAC Policy Based Architecture.

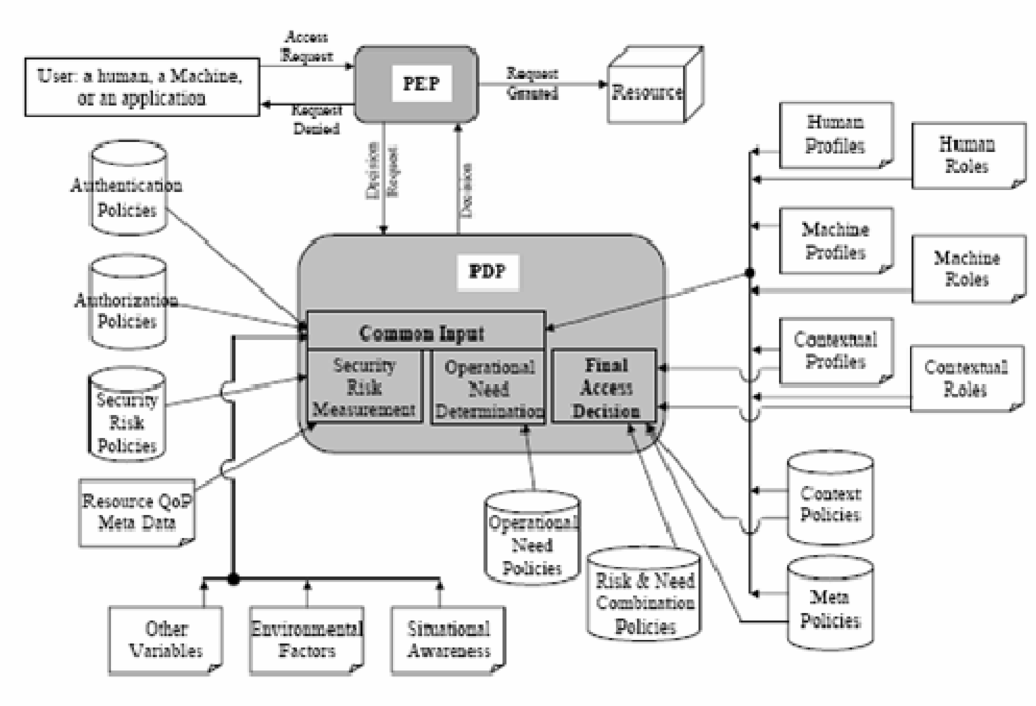


Figure 3. RAdAC PDP Policy Based Architecture (From: Choudhary, 2005)

The Policy Enforcement Point (PEP) is the point on a server that enforces policy decisions in response to a request from a user requesting access to a resource on a computer or network server (Yavatkar, Pendarakis, Guerin, 2000). The Policy Decision Point (PDP) is the point on a server that makes policy decisions in response to a request from a user wanting to access a resource on a computer or network server (Yavatkar, Pendarakis, Guerin, 2000). The PEP initiates communication between the two components. When the PEP receives a request that requires a policy decision it will formulate a policy decision request and send it to the PDP. The PDP returns the policy decision and the PEP is then responsible for enforcing it by either denying or accepting the original request. Common Open Policy Service (COPS) is the most common protocol used to communicate policy information between the PEP and PDP. COPS is a client/server protocol that provides transport services for moving policy information among IP network nodes (Sheldon, 2001).

The key to an effective PBM system is an effective policy (McGraw, 2006). A policy is a rule set governing an entity behavior. The rule set must be centrally defined and follow a common information model. A policy also has the following attributes: A scope, mechanism, an action, and a triggering event or condition (Martin, 1999). Historically, businesses have had conventional policies that were on paper and were simply the rules by which a company operates.

In order for PBM to work these policies must be automated and converted into digital polices. Digital policies are comprised of policy objects and policy elements that are able to be accessed by network components in real time. A policy object contains policy-related information such as policy elements and is carried in a request or response related to a resource access decision. A policy element contains single units of information necessary for the evaluation of policy rules. One policy element may carry user identification whereas another policy element may carry user credentials. The policy elements themselves are expected to be independent (Martin, 1999).

A PBM system will have many policies that work together to create a system that is capable of making complex decisions. The digital policies are organized into repositories, known as the policy information bases (PIB). The policies are retrieved via various servers such as those for the access control policy, authentication, authorization, and access rights. Policy retrieval uses standard interfaces such as the lightweight directory access protocol (LDAP) (Choudhary, 2005).

Figure 4 shows an example of the decision making process that occurs during a RAdAC transaction and illustrates the need for various policies to be accessed throughout the process.

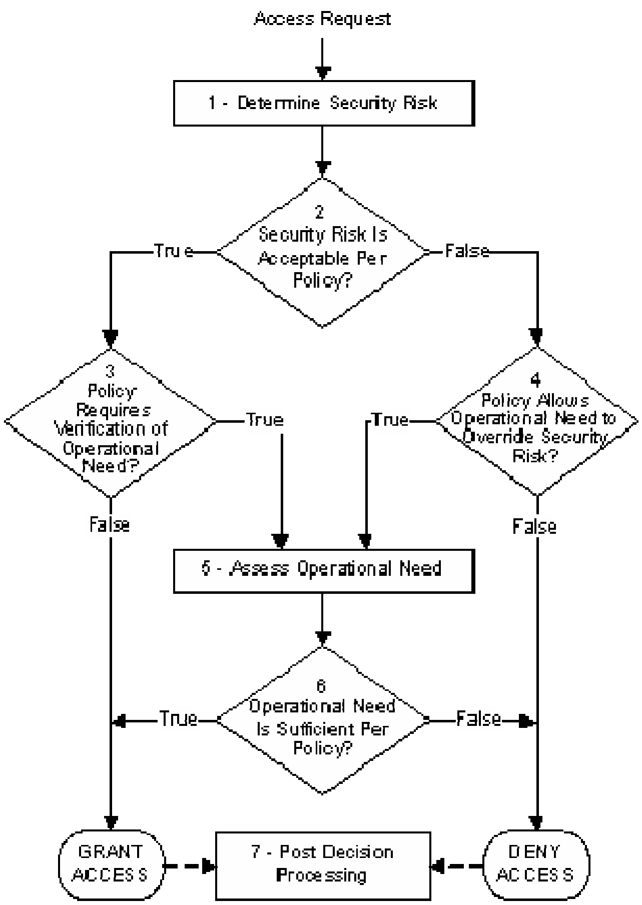

Access Request
1 - Determine Security Risk
2 Security Risk Is Acceptable Per Policy?
True
False
3 Policy Requires Verification of Operational Need?
True
False
4 Policy Allows Operational Need to Override Security Risk?
True
False
5 - Assess Operational Need
6 Operational Need Is Sufficient Per Policy?
True
False
GRANT ACCESS
7 - Post Decision Processing
DENY ACCESS

Figure 4. RAdAC Notional Process Model (From: McGraw, 2006)

6. RAdAC Policy Architecture

a. Security Risk Measurement Function

RAdAC incorporates a real time, probabilistic determination of security risk into the access control decision rather than just using a hard comparison of the attributes of the subject and object as in traditional models (McGraw, 2006). The security risk measurement function provides a quantitative assessment of the amount of risk associated with granting a requester access to a resource. Risk is introduced into each request from a variety of sources. The value of the information being accessed in conjunction with the trustworthiness of the requester, the protection level of the IT components, the current operational situation and the threat level of that environment along with the access history of each of these factors all contribute to the total security risk. Many types of digital policies will be needed to assist this function in determining a total security measurement (Choudhary, 2005). Digital policies will determine some quantitative level of risk associated with each of these factors as well as a quantitative level of total risk. These policies will also specify the acceptable level of risk for each risk factor and the total amount of acceptable risk.

b. Operational Need Determination Function

The function that determines operational need provides a quantifiable measure of the operational need associated with an access control decision. Historically, operational need was called "need to know" and was used as a way to restrict access instead of grant access. The RAdAC operational need determination function allows operational need to enable access if, under specified conditions, the operational need outweighs the security risk.

At this point in an information transaction the security risk has been determined. Digital policies would specify the requirements for determining the level of operational need, depending on whether the security risk was acceptable or unacceptable. Even if the security risks were acceptable there may be situations in which the requester has no operational need to access the information.

There may also be situations that the security risk was determined to be unacceptable but the requestor might have an operational need to access the information regardless of that risk. The digital policies used must be able to specify whether operational need may outweigh security risk, which areas of security risk operational need may take precedence over, and under what conditions (McGraw, 2005). Operational need digital policies must be able to describe the criteria and environment to assess how important the access decision is to the satisfactory performance of the system or mission operations. Factors such as the requestor's location, rank, mission or other situational factors might be used to determine a level of operational need that can outweigh the risk involved. In addition, these policies must also make use of all the information described in the security risk measurement (Choudhary, 2005).

c. Final Access Decision Function

The final access decision function makes the final determination on whether to grant access or not. It will take input from both the security risk measurement function and the operational need determination function. The digital policies used here will specify the acceptable levels of risk of individual components of the RAdAC process and the level of operational need required to outweigh those security risks.

Final access decision digital policies will specify the rules for access for various classes of information objects under different conditions (McGraw, 2006). The final access decision function uses a dynamic weighting system that incorporates real time environmental factors, situational factors, heuristics, and digital policies into every decision (Choudhary, 2005). The digital policies specify the relative weighting of these risk factors in computing a composite risk. A critical element to making the RAdAC model successful is effectively implementing and managing digital policies (McGraw, 2006). Figure 5 is a functional depiction of the factors that go into the final access decision in the RAdAC model.

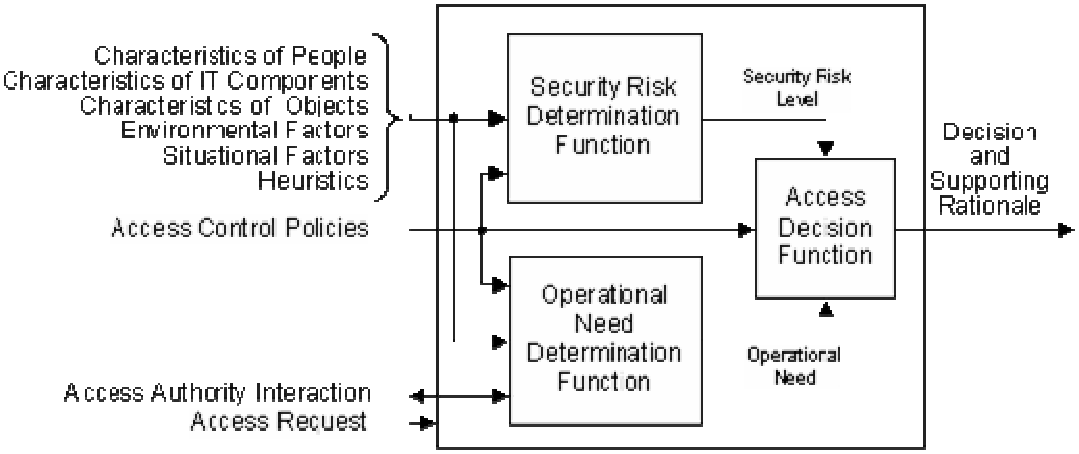

Characteristics of People
Characteristics of IT Components
Characteristics of Objects
Environmental Factors
Situational Factors
Heuristics
Access Control Policies
Access Authority Interaction
Access Request
Security Risk Determination Function
Security Risk Level
Access Decision Function
Operational Need Determination Function
Operational Need
Decision and Supporting Rationale

Figure 5. RAdAC Functional Depiction (From: McGraw, 2006)

III. RADAC RISK FACTORS

A. CHAPTER OVERVIEW

This chapter will provide an in-depth look at the NSA RAdAC risk factors. The NSA has identified six main risk categories: characteristics of the requester, characteristics of the IT components, situational factors, environmental factors, characteristics of the information requested and heuristics (McGraw, 2006). Each of these categories has a number of sub-factors that can be associated with them. This thesis has attempted to identify the most significant risk sub-factors that will have the greatest impact on each of the main categories.

B. CHARACTERISTICS OF REQUESTER

Characteristics of the requester are the risks associated with the person, machine or application that is requesting access to the data. The Jason Report identified several factors that should be examined that relate to the individual involved in the transaction (Horizontal Integration, 2004). This thesis addresses some of those factors and identifies several more. This risk category will consist of factors such as the person's role, rank, clearance level and education level. The purpose of this risk category is to assess how trustworthy the requester is. The higher the level of trust, the lower this risk value will be.

1. Role

This risk factor is associated with the requester's role within an organization. Typically, in the military, this would correspond to the requester's position of authority in that organization. Examples of this within the United States Navy include a Commanding Officer, an Executive Officer, a Department Head, a Division Officer and then service members.

In the scenario tested by this thesis, the assumption has been made that the higher a requester's role is within an organization the less likely they are to be a security risk. The opposite is true for the lower the requester's role. A new service member who has no position of authority will be more likely to commit a security violation whether through malice or negligence. With actual data, the opposite may be found to be true with a lower risk value assigned to a requester with a lower role.

2. Rank

Rank deals strictly with the risk associated the requester's relative position within a structured organization. Ranks in the military are divided between officers and enlisted. Officer ranks start at O-1 and go to O-10 while enlisted ranks range from E-1 to E-9.

Similar to the requester's role, the assumption has been made for testing purposes that the likelihood of occurrence decreases as the requester's rank increases, but again, actual statistics may prove this untrue.

3. Clearance Level

This risk factor is associated with the clearance level the requester holds. The most common clearances in the military are Top Secret, Secret, Confidential, and no clearance. Unlike role and rank, where it is speculated that risk is inversely proportional as the role and rank increase, actual procedures, guidelines and policies are followed to ensure risk is adequately measured and minimized before allowing clearances to be issued. The test values for this thesis follow the assumption that these risk mitigations have been used for higher clearance thresholds. The higher the clearance granted, the lower the assigned risk value.

4. Access Level

This risk factor is associated with the access level of the requestor. Typically access level is simply a "yes" or "no" question. This is referred to more commonly as "need to know." If the requester has been granted access to information, the risk would be lower than if the requester has not been granted access. However, risk could increase if the requester is granted access by a third party instead of the data owner.

5. Previous Violations

This risk factor takes account of any security violations the requester may have had in the past. If a requester has had a violation in the past, this would increase the risk of the transaction. If the requester has no record of previous violations, this would not necessarily lower the risk, but it would simply not add to it.

6. Education Level

This risk factor is associated with the amount of security related training or education the requester has received. Typically, the more security related training a requester has received the less likely that requester is to commit a security violation. Therefore, the security risk would be lower. Conversely, if a requester has not received any security training there is a higher possibility that a security violation could occur due to negligent action or inaction.

C. CHARACTERISTICS OF IT COMPONENTS

Characteristics of the IT Components have to do with the risk associated with every component in the information transaction path. This risk category will consist of factors such as the type of machines being used, the distance the information has to travel, including the number of hops it must go through, applications involved, the encryption type and level being used. The purpose of this risk category is to assess how safe the data will be in transit, the higher the level of protection, the lower the risk value.

1. Machine Type

This risk factor is associated with the type of machines involved in the information transaction. There are many different types of machines that could be involved in the transaction. The most common would be servers, desktops and portable digital assistants (PDA). Servers would tend to be the most secure machine, while a PDA would introduce a higher amount of risk because of the vulnerabilities it would be exposed to, including loss or theft.

2. Applications

This risk factor is associated with the applications involved in the information transaction. There are a large number of applications that exist, but they can be narrowed down to the most common ones that are used to access information. They can then be narrowed down even further by those that have been approved for use in DoD systems. The most common applications used in an information transaction would be a database query, a file share or a browser. Each of these applications would have different risk values associated with them.

3. Connection Type

This risk factor is associated with the physical connections that create the information path. There are two broad categories, wired and wireless. Both of these have several sub categories such as copper wire or fiber optic for wired transactions and 802.11 or HF and UHF for wireless transactions.

The lowest risk has been assigned to a fiber optic connection for a number of reasons inherent in fiber optic cable (Denning, 1999). The risk would increase as the connection introduces more points at which the information could be intercepted or if a less secure medium is introduced within the transaction path.

4. Authentication Type

This risk factor is linked to the type of authentication used by the requester to verify identity. There are currently only a few accepted methods to verify identity. The most secure way would use Public Key Infrastructure (PKI) and would have the lowest risk value. The least secure would be a simple username and password and would have the highest risk value. Other authentication methods include biometrics, tokens and certificates. Each authentication method has different risks associated with it including biometric false positives, lost tokens and the distribution of certificates.

5. Network

This risk factor is associated with the network that the information transaction occurs. Currently, the most widely used networks in DoD are the Internet, Unclassified but Sensitive Internet Protocol Router Network (NIPRNet), Secret Internet Protocol Router Network (SIPRNet) and Joint Worldwide Intelligence Communications System (JWICS). Each network employs different protection mechanisms and has different numbers of people who have access to the network. JWICS would be considered the most secure network because of the high level of protections in place and the low number of people who have access to the network. The Internet would have the highest risk value because of the large number of people who have access to it and because it provides a very low number of protection devices.

The future implementation of the GiG intends to bridge all of these networks into a single network; therefore, the risk value would be that of the least secure part the information transaction traverses. In the future, routing algorithms may take security risk into account when computing routes for various kinds of information flow. A route may be chosen purely on lowest risk rather than shortest path or least weight.

6. Encryption Level

This risk factor is associated with the level of encryption used to protect the information during transmission. There are many widely accepted types of encryption in use and each of the types has various levels normally set by the key length of the encryption. Examples include Public Key Encryption (PKE), Advanced Encryption Standard (AES) and Data Encryption Standard (DES). Each of these types of encryption provides different levels of protection and can also be implemented with key lengths ranging from 64 bits to 2024 bits. Various government agencies including NSA, National Institute of Standards and Technology (NIST) and Defense Information Systems Agency (DISA) all provide guidance about what encryption should be used in which environment.

7. Distance

The distance risk factor is associated with the distance between the requester and the information. Generally speaking, the further the information has to travel the more risk is introduced. If the requester and the information are in the same building this would represent the least amount of risk. If the requester and the information were in different countries, thousands of miles apart, this would have a much higher risk value. Physical distance is not the only factor either, the more hops the information has to travel through the higher the risk is with the transaction. Under certain circumstances a shorter distances may have a higher risk than a longer distance if the number of hops is greater.

D. SITUATIONAL FACTORS

Situational factor risk is associated with the situation surrounding the transaction itself. The Jason Report identified some factors included in this category (Horizontal Integration, 2004). This thesis addresses some of those factors and identifies several more. This risk category will consist of factors such as the mission role of the requester, the transaction type and the time sensitivity of the information. The purpose of this risk category is to assess the amount of risk associated with the transaction without regard to the data or requester.

1. Specific Mission Role

This risk factor is associated with the mission the requester is currently engaged in. The information that is being requested should directly relate to the mission of the requester. If there is a direct relationship, this could lower the risk of the transaction. A request for information that is not directly related to a mission would have a higher risk value.

2. Time Sensitivity of Situation

This risk factor is associated with how quickly the requester needs to have access to the data in order to complete a mission. In an urgent situation the requester may only have minutes to retrieve a piece of information and be able to act on it. This urgent situation would lower the overall risk value. If the requester is on a mission that does not have an urgent need to access the data the risk value would go up. The assumption made for this thesis is that once the situation is over the use of the information will no longer be needed, therefore the shorter the timeline of the situation the lower the risk value.

3. Transaction Type

This risk factor is associated with how the data is being accessed and what the intended use of the data may be. There are several methods of accessing data including queries, displays and copies. A simple query or one time event to see if a piece of information exists would have a lower risk than requesting a copy of that information.

4. Auditable or Non-auditable

This risk factor is associated with the ability to record who, where, when and how the information was accessed. An assumption is made that if the machines have the capability to log transactions they also have the capability to be remotely audited and the transaction data consolidated to a single database. If the requester is using equipment that is able to log the history associated with the information transaction, this will lower the risk value of the transaction. A request for information that comes from a piece of equipment that is not capable of logging would have a higher risk value.

5. Audience Size

This risk factor is associated with the expected number of individuals or machines that will see a copy of the requested data. A request for information that comes from a system that is capable of distributing that information to a large audience would have a high risk value. A request from a single user using a PDA would have a lower risk value because it is likely that user will be the only one to see that information.

E. ENVIRONMENTAL FACTORS

Environmental factors are risks associated with the environment surrounding the transaction itself and the increased likelihood of an adversary being able to exploit that transaction (Choudhary, 2005). This risk category will consist of factors such as the current location of the requester and the data. The purpose of this risk category is to assess the amount of risk associated with the transaction with regard to the environment.

1. Current Location

This risk factor is associated with the physical security of the current location of the requester. The requester could be located anywhere in the world and could be in a variety of locations within a certain area. The most common locations within the military are Sensitive Compartmented Information Facilities (SCIF), Secure Operation Centers, Operation Centers, Field Locations and open terminals. A SCIF is an extremely secure environment with little chance of the requested information being compromised while an open terminal in an Internet Café would be a non-secure location with a high chance of compromise. The regional location of the physical location also affects the risk value. For example, an Operation Center in Iraq will have a higher risk value than an Operation Center in the United States.

2. Threat Level

This risk factor is associated with the current threat level of the region of the world that the requester is located. There are various warning systems in use including, in the DoD, DEFCON, INFOCON and FPCON; for the United States, The Homeland Security Advisory System; and for the world, WATCHCON and SANS INFOCON (Guild, 2004). They all have threat levels ranging from Low to High. As the threat level of a location increases so will the risk value of the information transaction. Research is needed to evaluate each of the various warning systems and their applicability to RAdAC.

F. CHARACTERISTICS OF THE INFORMATION REQUESTED

Characteristics of the information requested is the risk associated with the information itself. This risk category will consist of factors such as the classification level of the data, the permissions of the data and other aspects of the data that are required to gain access to it. The purpose of this risk category is to assess how sensitive the information is. The more sensitive the information is the higher this risk value will be.

1. Classification Level

This risk factor is associated with the classification level of the data. The most common classification levels in the military are Top Secret, Secret, Confidential, For Official Use Only (FOUO) and Unclassified. There are other classification levels that fall within the above broader categories such as NATO Restricted, No Foreign, etc... The higher the data is classified the higher the risk value will be to access it. An information transaction that requests unclassified data would have a risk value near zero while a request for Top Secret information would be at the high end of the scale.

2. Encryption Level Required to Access

This risk factor is associated with the predetermined level of encryption that is required to access particular information. Certain kinds of information, regardless of its classification level, may require specific levels of encryption in order to access it (Choudhary, 2005). This factor is independent of the encryption that is actually being used. For example, data on a DoD website may require SSL encryption to access it even though the data is unclassified. The higher the encryption level required the higher the risk value for the transaction will be.

3. Network Classification Level

This risk factor is associated with network classification level required for the information to be transmitted. Generally, the classification of the data would determine this requirement. Data classified at the secret level would need to be transmitted on the SIPRNet or higher. In order for the GiG to function, data must be able to cross domains when needed. In this case, it is possible that secret data could transit across the NIPRNet or lower. The risk value for the transaction will increase as the network classification required increases, because the chance of a transmission over a lower classified network could increase.

4. Permission Level

This risk factor is associated with the permissions set on the data. The most common permissions are read only, writable or executable. An information transaction could have numerous other permissions that apply. Data might be tagged as only being able to be queried, displayed, or it might be able to be copied but not modified. The higher the permissions on the data the lower the risk value will be.

5. Time Sensitivity

This risk factor is associated with the time sensitivity of the data itself. Data can be either perishable or non-perishable. Data that is perishable can have varying degrees that are measured in time. Data could have an expected life of just minutes to hours, days or weeks. Data that is non-perishable is considered to be useful for a significant length of time, generally years or decades even. The risk value will be highest for non-perishable data and will decrease as the expected useful lifetime of the data decreases.

G. HEURISTICS

This risk category is associated with the amount of risk in a transaction based on similar transactions that have occurred before. This risk category will consist of a record of all transactions that have occurred and the risk value associated with them. The purpose of this risk category is to either lower or raise the risk value based on the history of similar transactions. The principles for this risk category is the concept of a Trust Management System that is able to learn the behavior of the components in a transaction and then predict what their future behavior will be (Adams & Davis, 2005).

1. Risk Knowledge

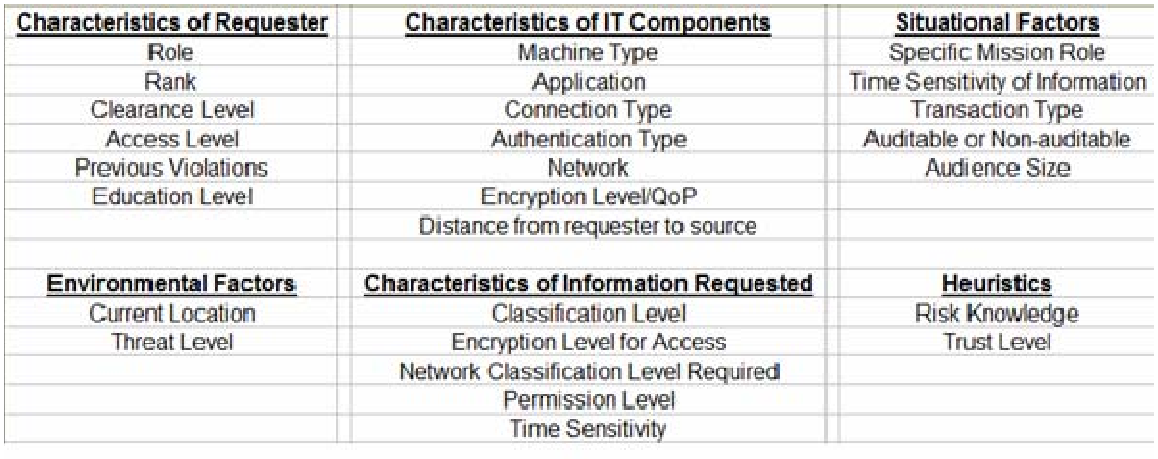
This risk factor is associated with any known previous security violations associated with the information transaction. Each unsuccessful information transaction will be recorded and will raise the risk value if those components are used in future transactions. Examples of this include a requester who is known to have misused data or an IT component that is known to have been compromised.

2. Trust Level

This risk factor is associated with a history of successful information transactions that have occurred. Each successful information transaction will build trust with the components of that transaction. The more successful transactions a requester, IT component, etc. has completed, the lower the risk value will be for future transactions involving those same components.

H. CONCLUSION

The NSA identified six main risk categories and this thesis identifies several risk factors for each category. This list is not intended to be all inclusive but rather the list represents those factors that we feel represent the most significant amounts of risk in an information transaction. Table 1 lists the identified risk factors.



Characteristics of Requester	**Characteristics of IT Components**	**Situational Factors**
Role	Machine Type	Specific Mission Role
Rank	Application	Time Sensitivity of Information
Clearance Level	Connection Type	Transaction Type
Access Level	Authentication Type	Auditable or Non-auditable
Previous Violations	Network	Audience Size
Education Level	Encryption Level/QoP	
	Distance from requester to source	
Environmental Factors	**Characteristics of Information Requested**	**Heuristics**
Current Location	Classification Level	Risk Knowledge
Threat Level	Encryption Level for Access	Trust Level
	Network Classification Level Required	
	Permission Level	
	Time Sensitivity	

Table 1. RAdAC Risk Factors

IV. QUANTIFICATION PROCESS

A. INTRODUCTION

This chapter will introduce and explain the quantification process used in the calculation of the Total Security Risk Measurement. It will start with the rationale for the simplified triangular distribution used to represent the data in the thesis. Next, the chapter will discuss the different levels of risk and provide a definition for low, medium and high probability of occurrence and consequence of occurrence. The chapter will also provide a discussion of a collection of expert's weightings. Finally, the chapter will present a brief explanation on Monte Carlo simulation and uncertainty, as well as an explanation of the Excel spread sheet and the calculations for individual risk factors and the Total Security Risk Measurement.

B. DATA

At this time there is no statistical data available for the risk factors to determine an actual distribution and form an accurate model. In order to demonstrate the process of computing a Total Security Risk Measurement a simplified triangular distribution was used in lieu of actual data points. In the future perhaps a real world statistical database will be available to the RAdAC engine via dynamic update, using XML data tagging (Choudhary, 2004).

During a general transaction, we assume that an individual inserts his Common Access Card on which his User Identity (UI) is stored. Every piece of information that is stored on his card including security clearance, secret keys, public keys, position in hierarchy, and user name is encoded and sent through the network. The Context Specification (CS), which includes the owner of the mission, the mission that the user is engaged in and the task within the mission will be tagged and sent through the network in the same manner to complete the Compound Identity (CI) (Choudhary, 2006). Concurrently, each node in the network will have its own metadata tag to be encapsulated in the datagram and will have its own specific risk numeric. The process continues through every identified risk factor to complete the risk measurement.

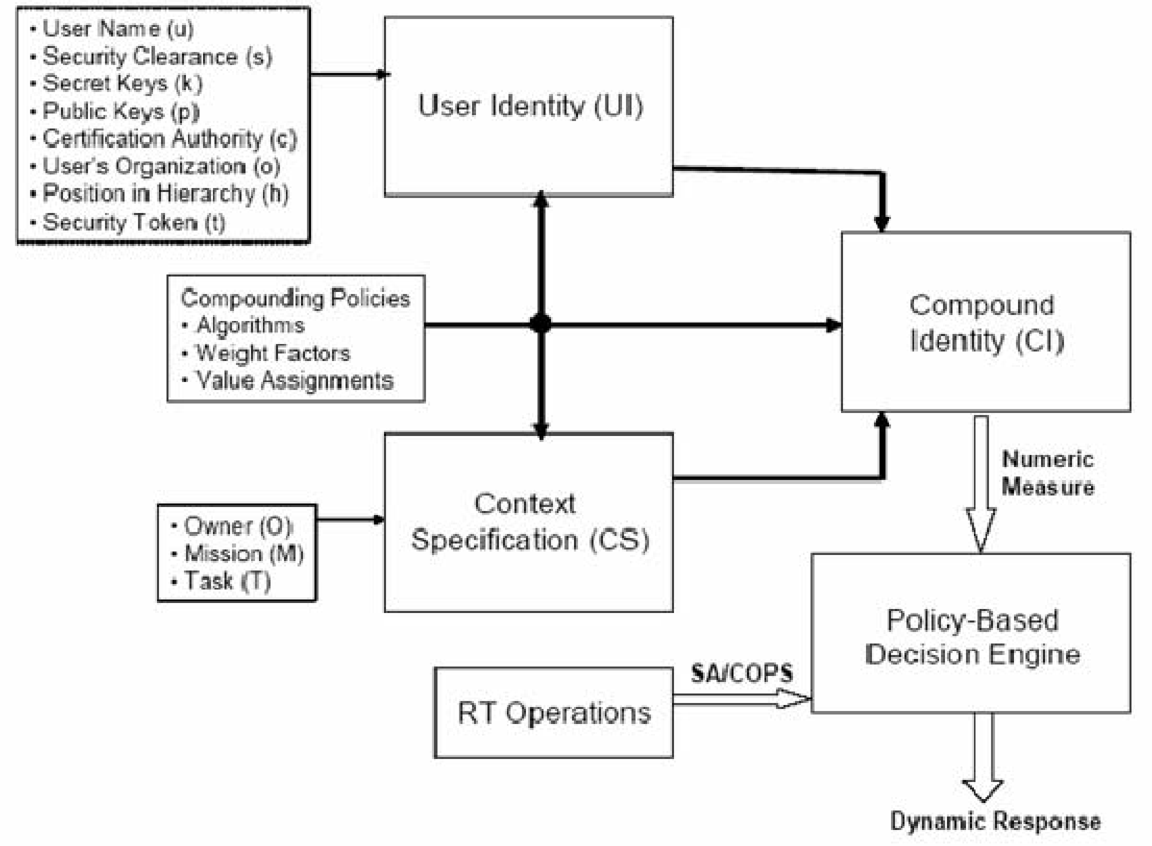


Figure 6. A Schematic View for Defining a Compound Identity (From: Choudhary, 2006)

C. PROBABILITY DISTRIBUTION

For the purpose of demonstrating the Total Security Risk Measurement process a simple triangular distribution was chosen. A triangular distribution has three underlying conditions: a specific minimum, a specific maximum and most likely value that falls somewhere between the minimum and maximum. The most likely value would occur more times than either the minimum or maximum thus forming a triangle (Mun, 2006).

The triangle distribution has been chosen for this thesis because the risk ranges, low, medium and high, fit the minimum and maximum conditions. When actual data becomes available a more appropriate distribution would be inserted in the place of the triangle distribution.

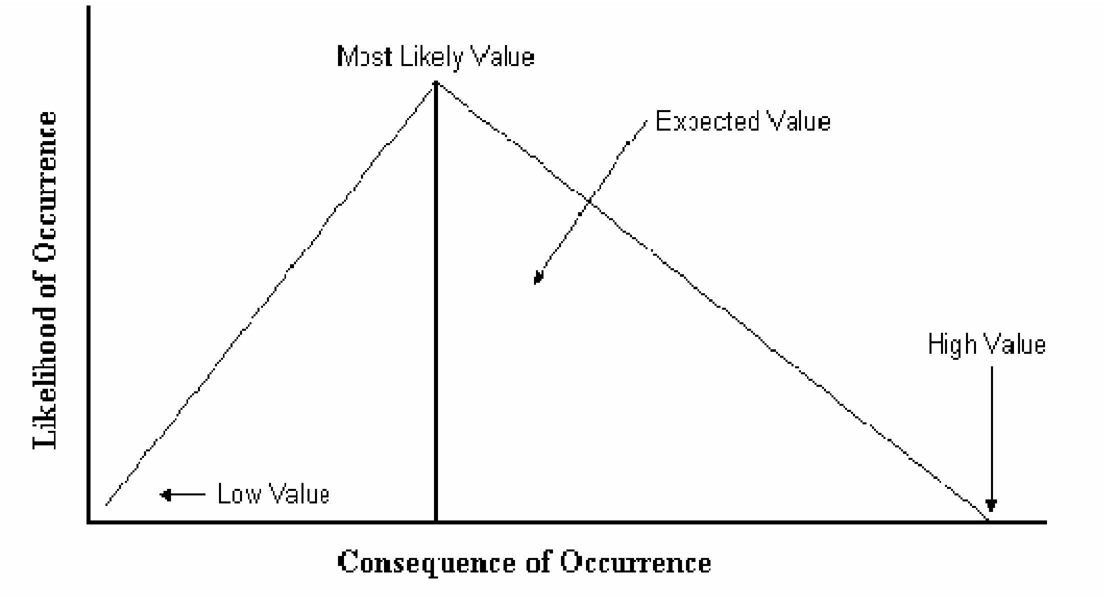


Figure 7. Example of a Triangle Distribution

D. DEFINITION OF RISK

The IA Pub 5239.16 (2003) defines risk as "a combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting impact."

1. Probability of Occurrence

a. High

The attack requires a minimal combination of effort and coincidence of events to succeed, and/or the threat-agent is both motivated and capable.

b. Medium

The attack requires moderate effort and coincidence of events to succeed. The threat-agent has some of the resources required and/or a moderate level of motivation.

c. Low

Countermeasures are in place to prevent or significantly impede successful exploitation, and/or the threat-agent lacks motivation or capability.

2. Consequence of Occurrence

The categories of the consequence of occurrence were given to the experts to provide a scale on which to base their opinion. They are not used further in this thesis.

a. High

Successful exploitation could result in substantial impact to the organization, including unavailability, modification, disclosure, or destruction of valued data or other system assets; loss of system services for an unacceptable period of time; or possible injury to or death of personnel.

b. Medium

Successful exploitation could result in moderate impact to the organization, such as discernable but recoverable unavailability, modification, disclosure, or destruction of data or other system assets or services.

c. Low

Unavailability, modification, disclosure, or destruction of data or degradation of system assets and services are easy to detect and correct, and impact to the organization is minor.

E. MONTE CARLO SIMULATION

Monte Carlo Simulation is a forecasting tool used to incorporate a level of uncertainty and randomness (Mun, 2006). Like rolling the dice repeatedly to see what combinations will appear, Monte Carlo simulation will run a predefined probability distribution through a function a preset number of times to provide a forecast. The initial input variable is randomly selected from the probability distribution and run through the given formula which calculates a single outcome for the uncertain variable. This process is repeated a specified number of times and the results are then tabulated. The tabulated results will imitate the initial input assumption distribution (Mun, 2006).

Computing technology has become increasingly powerful with the number of iterations and the complexities that computers can calculate. The power in any simulation is being able to make better decisions about future uncertainties when real-life models would be too complex or expensive to reproduce (Mun, 2006).

F. EXPERT OPINION

We asked security experts to assign a weight for the potential damage done for a security violation associated with a risk factor or factors. They were chosen from various fields to provide different viewpoints and to flush out areas of concern that may not be thought of by polling experts in only one specific area. The experts have been selected from fields including business, information assurance, physical security and computer science. Due to time constraints we were only able to interview a small number of experts. In order for the model to be useful in a real world situation a much larger number of experts in each field would need to be interviewed. The results would then need to be analyzed to create an appropriate set of statistics that could be used. Further discussion on this is included in Chapter VI.

The experts we interviewed were given a list of the risk categories followed by each of the risk factors in that category. They were asked to weight each of the six main risk categories totaling 100 percent with a higher weight representing more potential damage. They were then asked to break down each of the individual risk factors using the same method.

In the future, these weights will be policy driven and will require constant review for new threats and vulnerabilities. There could also be multiple weight sets active varied by region or terror threat level.

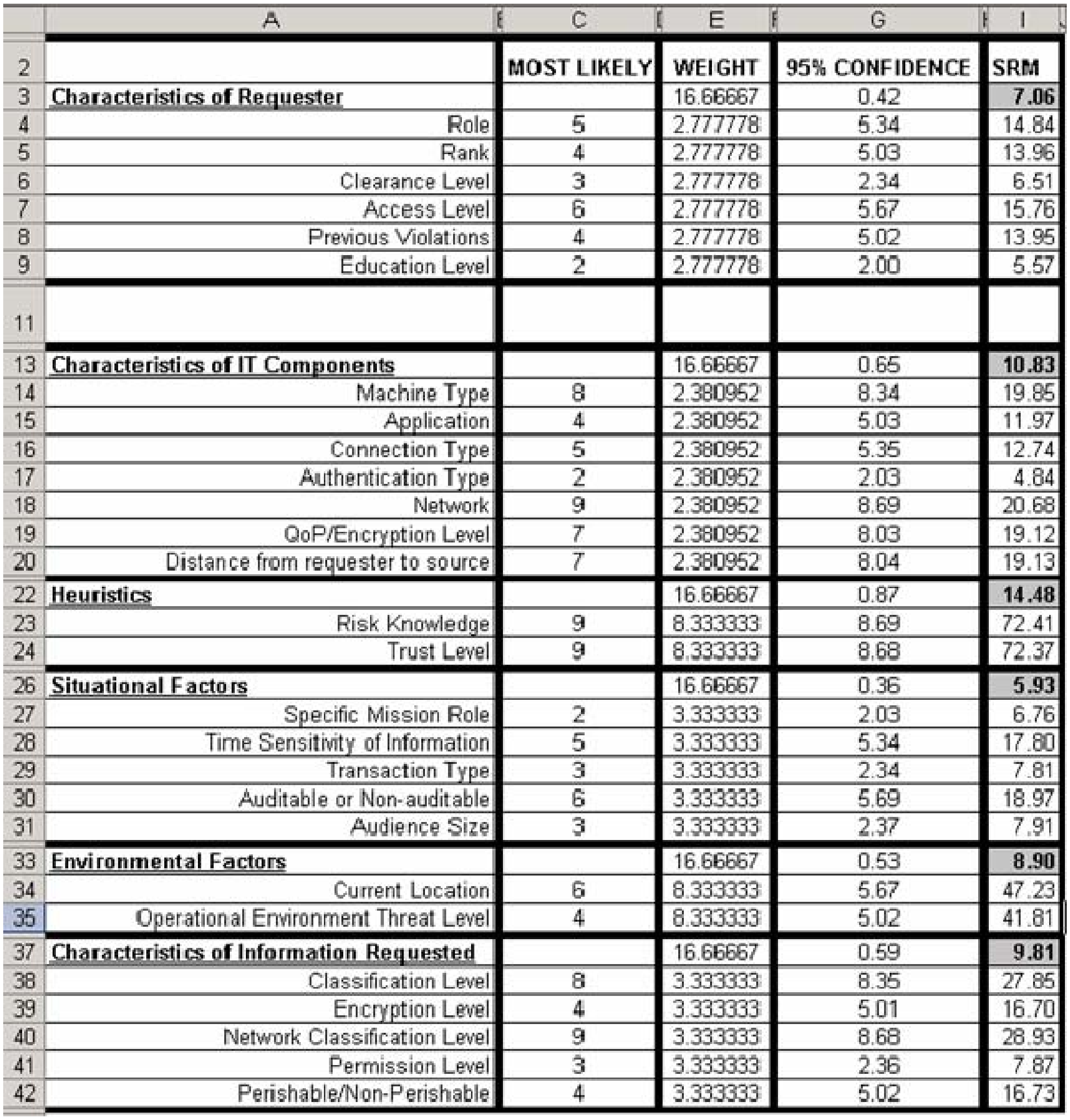
G. EXCEL SPREADSHEET EXPLANATION

An Excel Spreadsheet was used to build a model that represents the security measurement function of the RAdAC engine. The spread sheet has two main parts, the first is a Total Security Risk Measurement Sheet and the second is a collection of individual risk factor sheets. The model works by first calculating a most likely value for each of the risk factors and then applying a weighting against the values. The weighted values are then summed up to create the Total Security Risk Measurement. A more detailed explanation of the spreadsheet follows.

1. Total Security Risk Measurement Sheet

The Total Security Risk Measurement (TSRM) Sheet is shown in Table 2. The risk categories and individual risk factors are listed in Column A. Column C is the most likely value for each transaction. The most likely value is transferred to the appropriate level (High, Medium, or Low) to run through the Monte Carlo simulation on the subsequent individual risk factor sheets. The input for Column E titled “WEIGHT” comes directly from the expert opinion results. Column G returns the 95% Confidence

Level calculated from the Monte Carlo simulation. Column I is the Security Risk Measurement for each of the individual risk factors and is tallied for a Category Risk Measurement.



	A	C	E	G	I
2		MOST LIKELY	WEIGHT	95% CONFIDENCE	SRM
3	Characteristics of Requester		16.66667	0.42	7.06
4	Role	5	2.777778	5.34	14.84
5	Rank	4	2.777778	5.03	13.96
6	Clearance Level	3	2.777778	2.34	6.51
7	Access Level	6	2.777778	5.67	15.76
8	Previous Violations	4	2.777778	5.02	13.95
9	Education Level	2	2.777778	2.00	5.57
11					
13	Characteristics of IT Components		16.66667	0.65	10.83
14	Machine Type	8	2.380952	8.34	19.85
15	Application	4	2.380952	5.03	11.97
16	Connection Type	5	2.380952	5.35	12.74
17	Authentication Type	2	2.380952	2.03	4.84
18	Network	9	2.380952	8.69	20.68
19	QoP/Encryption Level	7	2.380952	8.03	19.12
20	Distance from requester to source	7	2.380952	8.04	19.13
22	Heuristics		16.66667	0.87	14.48
23	Risk Knowledge	9	8.333333	8.69	72.41
24	Trust Level	9	8.333333	8.68	72.37
26	Situational Factors		16.66667	0.36	5.93
27	Specific Mission Role	2	3.333333	2.03	6.76
28	Time Sensitivity of Information	5	3.333333	5.34	17.80
29	Transaction Type	3	3.333333	2.34	7.81
30	Auditable or Non-auditable	6	3.333333	5.69	18.97
31	Audience Size	3	3.333333	2.37	7.91
33	Environmental Factors		16.66667	0.53	8.90
34	Current Location	6	8.333333	5.67	47.23
35	Operational Environment Threat Level	4	8.333333	5.02	41.81
37	Characteristics of Information Requested		16.66667	0.59	9.81
38	Classification Level	8	3.333333	8.35	27.85
39	Encryption Level	4	3.333333	5.01	16.70
40	Network Classification Level	9	3.333333	8.68	28.93
41	Permission Level	3	3.333333	2.36	7.87
42	Perishable/Non-Perishable	4	3.333333	5.02	16.73

Table 2. Total Security Risk Measurement (TSRM) Sheet

a. Factor and Category Security Risk Measurement Calculations

The IA Risk Assessment process as defined by Kenneth Montry (2005) of the Boeing Company calculates risk by multiplying the probability of occurrence (Most

Likely Value) by the consequence of occurrence (Weight). The same technique has been used in this thesis. Each of the Factor Security Risk Measurements is calculated by multiplying the Expert Weight in column E by the 95% Confidence Level in column G. The risk factors under each of the risk categories are then summed to provide the Category Security Risk Measurement. Figure 8 is a graphical representation of each of the risk categories.

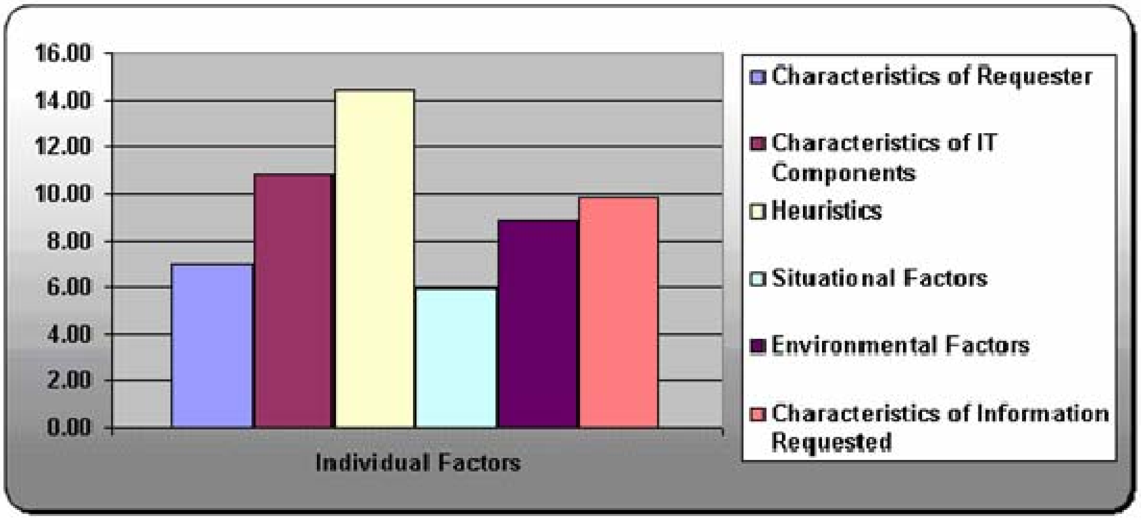


Figure 8. Graphical Representation of Risk Categories

(1) The "Most Likely Value" is a numeric value based on information compromise statistics. It is not a one-for-one value based on the number of violations taking place. Rather, the statistic will be classified from 0.00 to 10.00 based on a relative floating scale. The more often an incident takes place and can be attributed to a particular risk factor or factors, the higher the most likely value will be for that particular factor. For example, if an information compromise due to a particular risk factor happens once out of every 100,000 transactions and is given a "most likely value" of 10.00. If the same event occurs once out of every 500,000 transactions it could also be given a "most likely value" 10.00 if the relative scale has changed.

(2) The "Weight" refers to the potential impact or damage that could be caused by an information compromise occurring due to a particular risk factor.

A higher number represents more potential damage. A lower number signifies less potential damage. The weight sets were established by the individual experts polled for the thesis.

b. Total Security Risk Measurement Calculation

The Total Security Risk Measurement is a sum of the Category Security Risk Measurements. The total returned will be between 0.00% and 100.00%. Figure 9 represents the Total Security Risk Measurement which contains the final summation of all of the risk categories.

Total Security Risk Measurement

57.01

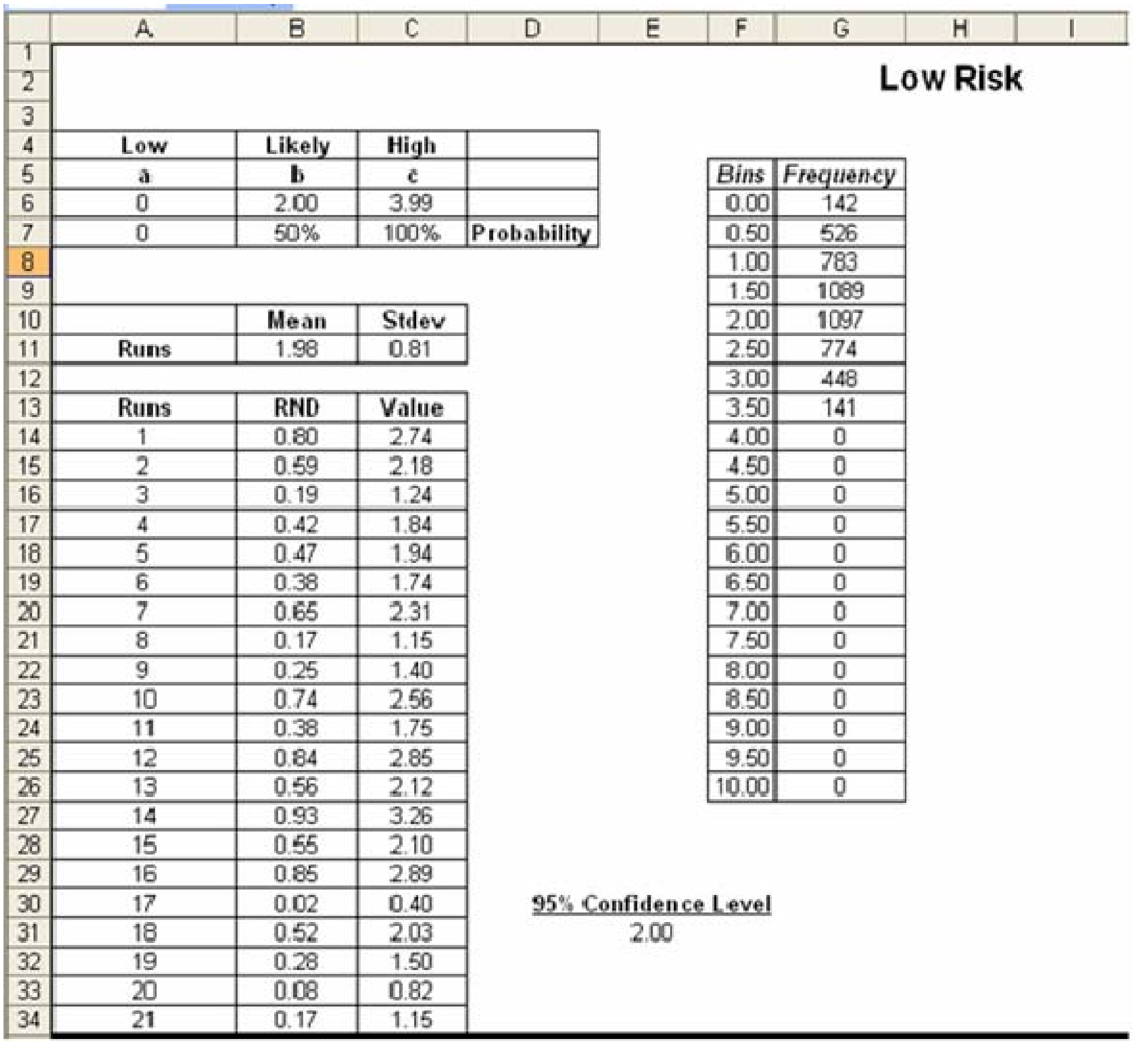
Figure 9. Total Security Risk Measurement

2. Individual Risk Factor Sheets

Following the TSRM sheet are the individual risk factor sheets. Table 3 shows an example. Each sheet runs the most likely value through the triangle distribution and the Monte Carlo simulation for the individual risk factors. The 95% confidence level is then returned to the TSRM sheet. The risk factor sheets are broken into three sections in order from low risk to high risk. The "Low" risk falls between 0.00 and 3.99. The "Medium" range is between 4.00 and 6.99 and the "High" risk range will 7.00 and 10.00. The "Most Likely Value" will be placed in the appropriate risk range with a simple IF/THEN statement. The two sections not being used will not calculate or return anything to the TSRM sheet and will appear invalid.

In each one of the sections, from Row 4 to Row 7, the upper left table containing "Low," "Likely," and "High" defines the risk range. The "Low" and "High" values are constant throughout each of the risk factors and represent the minimum and maximum conditions defined for the triangular distribution.

The “Likely” input corresponds to the matching risk factor “Most Likely Value” in the TSRM sheet. Row 7 defines the cumulative probability. In Row 11, the mean calculates the average of the 5,000 iterations with the standard deviation displayed to the right. The final table represents the 5,000 trials. Column A defines the trial number. Column B chooses a random number through the Excel RAND() function. Column C then uses that random number in the triangular distribution formula (Hesse, 2000).



Low Risk

Low	Likely	High	
a	b	c	
0	2.00	3.99	
0	50%	100%	Probability

	Mean	Stdev
Runs	1.98	0.81

Runs	RND	Value
1	0.80	2.74
2	0.59	2.18
3	0.19	1.24
4	0.42	1.84
5	0.47	1.94
6	0.38	1.74
7	0.65	2.31
8	0.17	1.15
9	0.25	1.40
10	0.74	2.56
11	0.38	1.75
12	0.84	2.85
13	0.56	2.12
14	0.93	3.26
15	0.55	2.10
16	0.85	2.89
17	0.02	0.40
18	0.52	2.03
19	0.28	1.50
20	0.08	0.82
21	0.17	1.15

Bins	*Frequency*
0.00	142
0.50	526
1.00	783
1.50	1089
2.00	1097
2.50	774
3.00	448
3.50	141
4.00	0
4.50	0
5.00	0
5.50	0
6.00	0
6.50	0
7.00	0
7.50	0
8.00	0
8.50	0
9.00	0
9.50	0
10.00	0

95% Confidence Level

2.00

Table 3. Individual Risk Factor Sheet

The Monte Carlo simulation accounts for uncertainty and provides a forecast or confidence level used by the rest of the model. For example, if the Previous Violations factor has been given a most likely value of 2.00 it would be placed in the low risk range.

The lowest possible value in that range is 0.00 and the highest is 3.99. This is shown in Row 6 of Table 3. The Monte Carlo simulation will run through 5,000 iterations of the formula with the triangle distribution returning 5,000 numbers between 0.00 and 3.99 under the “Value” column. The results are tabulated and placed into standard histogram form with bins in increments of 0.5.

Even though the most likely value is 2.00 based on a combination of historical and near real-time data, it cannot be known that it will always be that value. The Monte Carlo simulation will calculate how many times the value will be lower than 2.00 and how many times it will be higher than 2.00. Given the newly calculated distribution it can be determined with a confidence level that the risk factor will be below a certain number. In this example the result is 2.00 and is shown in Column E, Row 31 of Table 3.

V. EXPERIMENT RESULTS

A. INTRODUCTION

This chapter will document the results of our evaluation of the TSRM model using individual information transactions that will test the accuracy of the model. Three information transaction scenarios have been selected to test the lower, middle and upper bounds. Specifically, each of the scenarios will be tested against each of the expert opinion weightings and should return an appropriate TSRM number for the given situation.

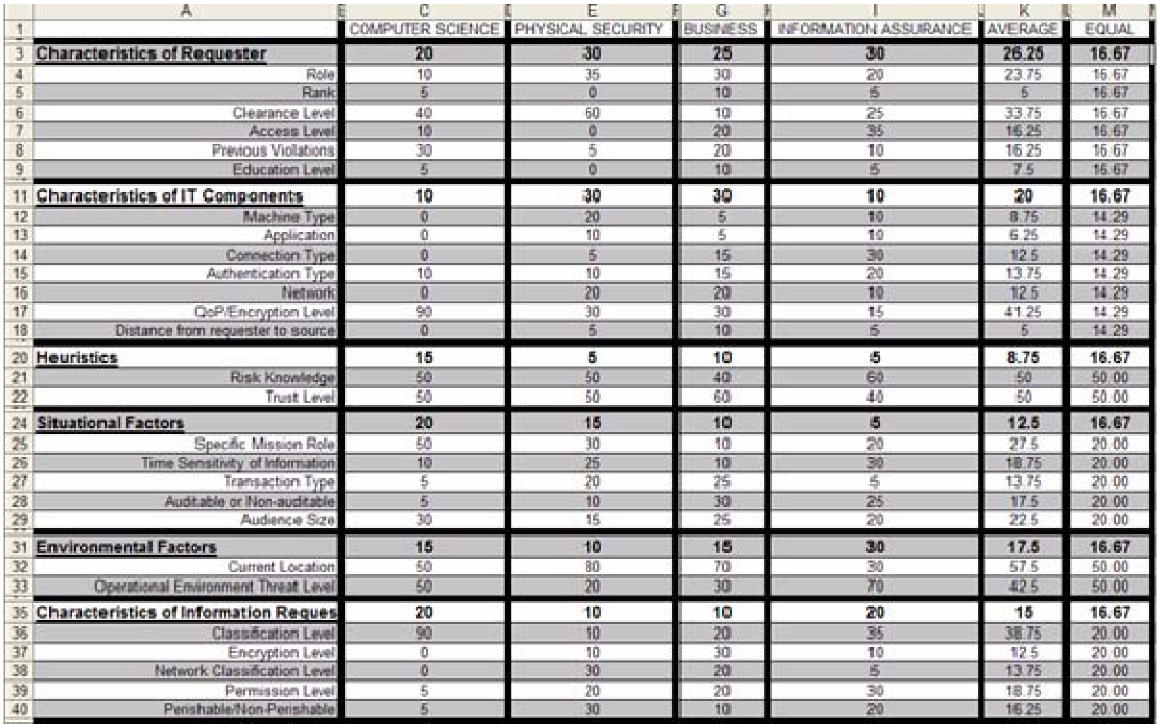
This chapter first presents the expert weight sets in an Excel spreadsheet with the obtained results and a short explanation. Following the weight sets, each of the scenarios is described in detail and given arbitrary most likely values that correspond to the situation to be placed in the model for testing. Finally, each of the three scenarios was applied to the TSRM model against each of the expert weight sets. The results will be presented individually and discussed.

B. EXPERT WEIGHT SETS

1. Explanation of the Excel Spreadsheet

Experts in the fields of Computer Science, Physical Security, Business and Information Assurance were asked to give their opinion on a weighting of the identified RAdAC risk factors. Table 4, Columns C through I, represent the four experts weight sets from the different fields, while Column K and Column M represent the average of the four expert weight sets and an equal weighting respectively. These final two categories provide baseline results from which a few observations will be made.

The percentages in the risk categories, shown in bold, sum up to 100 percent in each column with a higher weighting specified to those categories deemed to have a higher potential impact in the event of an information compromise. The risk factors under each risk category equal 100 percent in the same manner. If the risk factor equals zero, the expert did not feel that particular risk factor was relevant. These will be explained later in the individual results.



	A	C	E	G	I	K	M
1		COMPUTER SCIENCE	PHYSICAL SECURITY	BUSINESS	INFORMATION ASSURANCE	AVERAGE	EQUAL
3	**Characteristics of Requester**	**20**	**30**	**25**	**30**	**26.25**	**16.67**
4	Role	10	35	30	20	23.75	16.67
5	Rank	5	0	10	5	5	16.67
6	Clearance Level	40	60	10	25	33.75	16.67
7	Access Level	10	0	20	35	16.25	16.67
8	Previous Violations	30	5	20	10	16.25	16.67
9	Education Level	5	0	10	5	7.5	16.67
11	**Characteristics of IT Components**	**10**	**30**	**30**	**10**	**20**	**16.67**
12	Machine Type	0	20	5	10	8.75	14.29
13	Application	0	10	5	10	6.25	14.29
14	Connection Type	0	5	15	30	12.5	14.29
15	Authentication Type	10	10	15	20	13.75	14.29
16	Network	0	20	20	10	12.5	14.29
17	QoP/Encryption Level	90	30	30	15	41.25	14.29
18	Distance from requester to source	0	5	10	5	5	14.29
20	**Heuristics**	**15**	**5**	**10**	**5**	**8.75**	**16.67**
21	Risk Knowledge	50	50	40	60	50	50.00
22	Trust Level	50	50	60	40	50	50.00
24	**Situational Factors**	**20**	**15**	**10**	**5**	**12.5**	**16.67**
25	Specific Mission Role	50	30	10	20	27.5	20.00
26	Time Sensitivity of Information	10	25	10	30	18.75	20.00
27	Transaction Type	5	20	25	5	13.75	20.00
28	Auditable or Non-auditable	5	10	30	25	17.5	20.00
29	Audience Size	30	15	25	20	22.5	20.00
31	**Environmental Factors**	**15**	**10**	**15**	**30**	**17.5**	**16.67**
32	Current Location	50	80	70	30	57.5	50.00
33	Operational Environment Threat Level	50	20	30	70	42.5	50.00
35	**Characteristics of Information Reques**	**20**	**10**	**10**	**20**	**15**	**16.67**
36	Classification Level	90	10	20	35	38.75	20.00
37	Encryption Level	0	10	30	10	12.5	20.00
38	Network Classification Level	0	30	20	5	13.75	20.00
39	Permission Level	5	20	20	30	18.75	20.00
40	Perishable/Non-Perishable	5	30	10	20	16.25	20.00

Table 4. Summary of Expert Weightings

2. Results of Expert Weighting Opinion by Category

The weightings given by the experts provided quite different results. Further study would be useful to determine if several experts in the same field shared similar views. Additional research in this area could help understand if the differences were based on the individual, the field of study or a combination of both. The results we obtained are explained below.

a. Characteristics of Requester

The results for this category ranged from 20% to 30%. The computer science expert placed the least emphasis while the information assurance and physical security experts both placed the highest weightings.

b. Characteristics of IT Components

The results for this category were either 10% or 30%. The computer science expert and information assurance experts placed the least emphasis while the business and physical security experts both placed the highest weightings.

c. Heuristics

The results for this category ranged from 5% to 15%. The physical security and information assurance experts placed the least emphasis while the computer science expert placed the highest weighting.

d. Situational Factors

The results for this category ranged from 5% to 20%. Each of the experts chose a different weight for this category. The information assurance expert placed the least emphasis while the computer science expert placed the highest weighting.

e. Environmental Factors

The results for this category ranged from 10% to 30%. The physical security expert placed the least emphasis while the information assurance expert placed the highest weighting. The computer science and business experts both agreed at 15%.

f. Characteristics of Information Requested

The results for this category were either 10% or 20%. The computer science expert and information assurance experts placed the most emphasis on this factor while the business and physical security experts both placed the lowest weightings.

3. Results of Expert Weighting Opinion by Field

a. Computer Science

This expert placed the least emphasis on the Characteristics of IT Components with a weighting of 10%. The highest emphasis was put on Characteristics of Requester, Situational Factors and Characteristics of Information Requested all tied at 20%. The Heuristics weighting was set at 15% and Situational Factors at 20%, both of which were the highest of all the experts.

b. Physical Security

This expert placed the least emphasis on Heuristics with a weighting of 5%. The highest emphasis was put on Characteristics of Requester and Characteristics of IT Components both tied at 30%. The Environmental Factors category had a weight of 10% which was the lowest of all the experts.

c. Business

This expert placed the least emphasis on Heuristics, Situational Factors and Characteristics of Information Requested all tied with a weighting of 10%. The highest emphasis was put on Characteristics of IT Components at 30%. Overall these weightings were either tied with or in the middle of the expert's results.

d. Information Assurance

This expert placed the least emphasis on Heuristics and Situational Factors both with a weighting of 5%. The highest emphasis was put on Characteristics of Requester and Environmental Factors both at 30%. The Situational Factors category with a weight of 5% was the lowest of all the experts. The Environmental Factors category with a weight of 30% was the highest of all the experts.

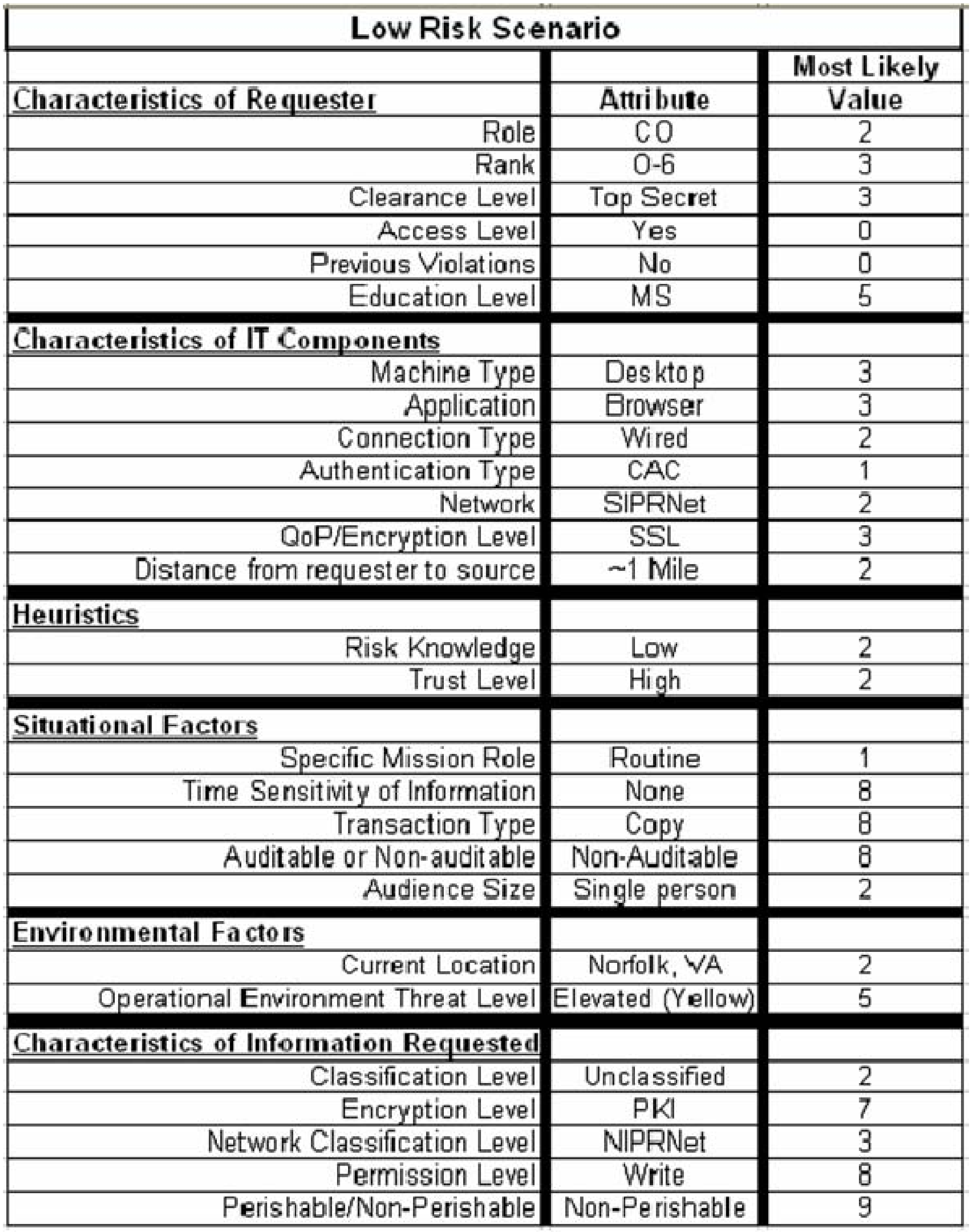
C. LOW RISK SCENARIO, TESTS AND OBSERVATIONS

1. Low Risk Test Scenario

A Navy Captain, sitting at his desk in Norfolk, VA, requests a file from another command also located in Norfolk. The Captain has a Top Secret clearance with no previous security violations. The information requested will be used for the normal operations of his command. The information is able to be copied, is non-perishable and non-auditable. The information will only be viewed by the Captain but he has permission to write and copy. The information is unclassified and is located on a DoD SIPRNet website that requires PKI Authentication.

2. Low Risk Most Likely Value Inputs

These numbers have been chosen arbitrarily throughout the scenario. They are based strictly on what we feel would be an appropriate risk value. Further research is needed to generate accurate inputs for this model. These numbers represent the most likely value in the triangle distribution portion of the TSRM model for the low risk scenario.



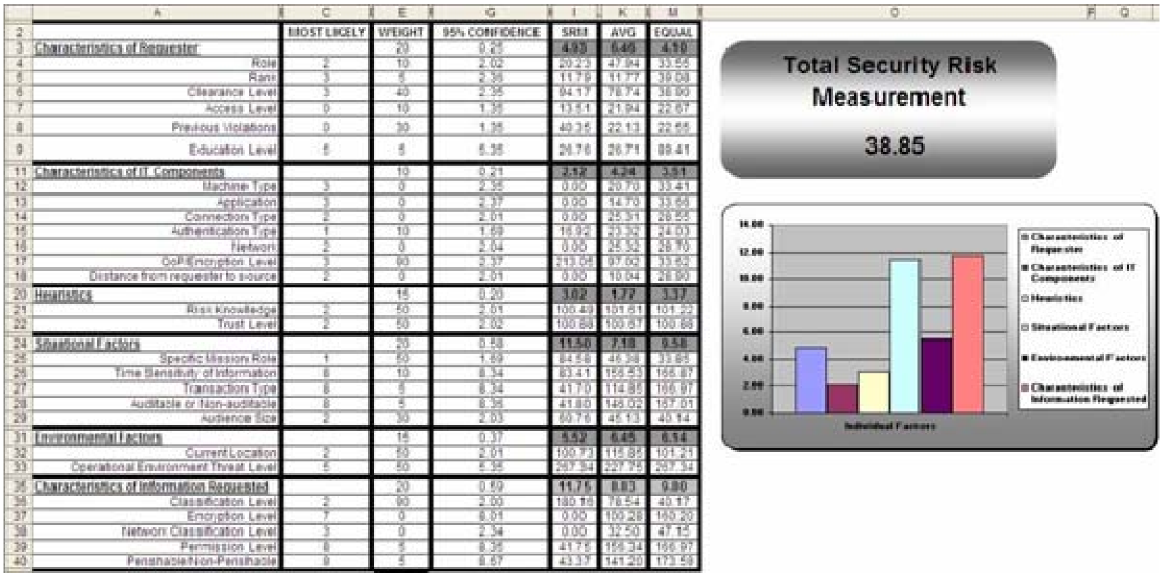
Low Risk Scenario		
		Most Likely
Characteristics of Requester	Attribute	Value
Role	CO	2
Rank	O-6	3
Clearance Level	Top Secret	3
Access Level	Yes	0
Previous Violations	No	0
Education Level	MS	5
Characteristics of IT Components		
Machine Type	Desktop	3
Application	Browser	3
Connection Type	Wired	2
Authentication Type	CAC	1
Network	SIPRNet	2
QoP/Encryption Level	SSL	3
Distance from requester to source	~1 Mile	2
Heuristics		
Risk Knowledge	Low	2
Trust Level	High	2
Situational Factors		
Specific Mission Role	Routine	1
Time Sensitivity of Information	None	8
Transaction Type	Copy	8
Auditable or Non-auditable	Non-Auditable	8
Audience Size	Single person	2
Environmental Factors		
Current Location	Norfolk, VA	2
Operational Environment Threat Level	Elevated (Yellow)	5
Characteristics of Information Requested		
Classification Level	Unclassified	2
Encryption Level	PKI	7
Network Classification Level	NIPRNet	3
Permission Level	Write	8
Perishable/Non-Perishable	Non-Perishable	9

Table 5. Low Risk Scenario Most Likely Values

3. Low Risk Scenario Test Results

a. Computer Science Expert

The Computer Science weighting returned the highest overall TSRM at 38.85. In general, the Computer Science expert felt that if the encryption was good enough, then machine type, distance, application, connection type and the network were irrelevant. In this scenario the encryption level was good enough to have a low risk value so the risk for the Characteristics of IT components was low. The Characteristics of the Information Requested risk category was above both the average and equal weightings even though the classification level of the information was unclassified. This is due to the high level of emphasis put on the Classification Level, in this case 90%.



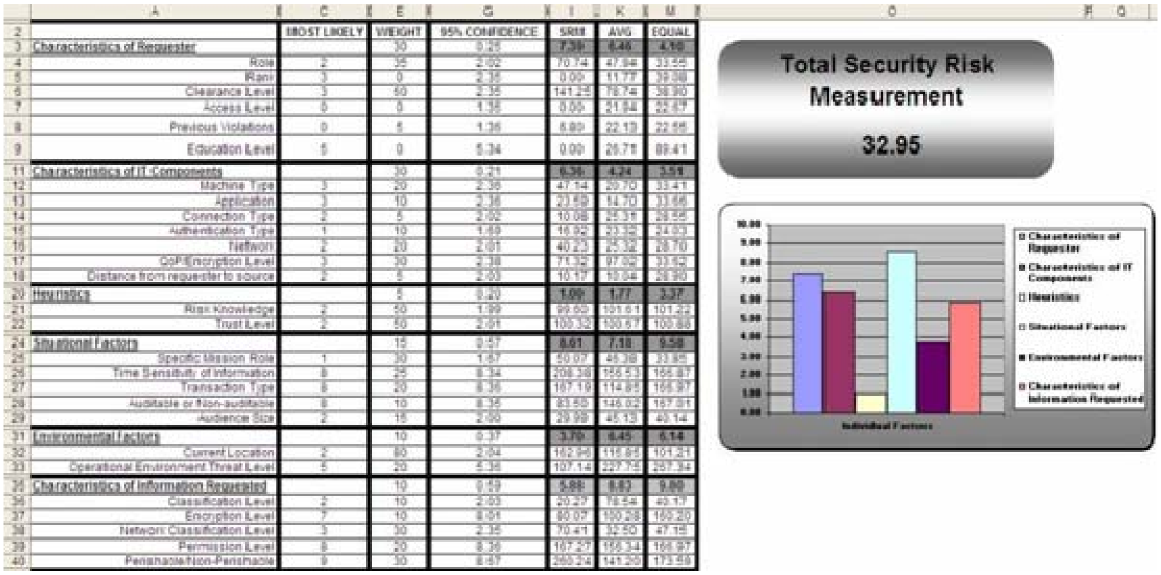
	A	C	E	G	I	K	M
2		MOST LIKELY	WEIGHT	95% CONFIDENCE	SRM	AVG	EQUAL
3	Characteristics of Requester		20	0.25	4.93	6.46	4.10
4	Role	2	10	2.02	20.23	47.84	33.56
5	Rank	3	5	2.36	11.79	11.77	39.08
6	Clearance Level	3	40	2.35	94.17	78.74	38.90
7	Access Level	0	10	1.35	13.51	21.94	22.67
8	Previous Violations	0	30	1.35	40.35	22.13	22.55
9	Education Level	6	5	5.35	26.76	26.71	89.41
11	Characteristics of IT Components		10	0.21	2.12	4.24	3.51
12	Machine Type	3	0	2.35	0.00	20.70	33.41
13	Application	3	0	2.37	0.00	14.70	33.66
14	Connection Type	2	0	2.01	0.00	25.31	28.55
15	Authentication Type	1	10	1.69	16.92	23.32	24.03
16	Network	2	0	2.04	0.00	25.32	28.70
17	OoP/Encryption Level	3	90	2.37	213.05	97.02	33.62
18	Distance from requester to source	2	0	2.01	0.00	10.04	28.90
20	Heuristics		15	0.20	3.02	1.77	3.37
21	Risk Knowledge	2	50	2.01	100.49	101.61	101.22
22	Trust Level	2	50	2.02	100.88	100.67	100.88
24	Situational Factors		20	0.58	11.50	7.18	9.58
25	Specific Mission Role	1	50	1.69	84.56	46.38	33.85
26	Time Sensitivity of Information	8	10	8.34	83.41	156.53	166.87
27	Transaction Type	8	5	8.34	41.70	114.85	166.97
28	Auditable or Non-auditable	8	5	8.36	41.80	146.02	167.01
29	Audience Size	2	30	2.03	60.76	45.13	40.54
31	Environmental Factors		15	0.37	5.52	6.45	6.14
32	Current Location	2	50	2.01	100.73	115.85	101.21
33	Operational Environment Threat Level	5	50	5.35	267.34	227.75	267.34
35	Characteristics of Information Requested		20	0.59	11.75	8.83	9.80
36	Classification Level	2	90	2.00	180.18	78.54	40.17
37	Encryption Level	7	0	8.01	0.00	100.28	160.20
38	Network Classification Level	3	0	2.34	0.00	32.50	47.15
39	Permission Level	8	5	8.35	41.75	156.34	166.97
40	Perishable/Non-Perishable	9	5	8.67	43.37	141.20	173.59

O
P
Q
Total Security Risk Measurement
38.85
14.00
12.00
10.00
8.00
6.00
4.00
2.00
0.00
Individual Factors
Characteristics of Requester
Characteristics of IT Components
Heuristics
Situational Factors
Environmental Factors
Characteristics of Information Requested

Table 6. Low Risk Scenario Computer Science Expert Results

b. Physical Security Expert

The Physical Security weightings came in with the second lowest TSRM at 32.95. A low emphasis placed on the Environmental Factors and Characteristics of the Information Requested, both 10%, resulted in the risk being lower than the average. The risk associated with Characteristics of IT Components was higher than normal because of the 30% weighting assigned to it. The other categories were in line with the average.



	A	C	E	G	I	K	M
2		MOST LIKELY	WEIGHT	95% CONFIDENCE	SRM	AVG	EQUAL
3	Characteristics of Requester		30	0.25	7.39	6.46	4.10
4	Role	2	35	2.02	70.74	47.94	33.55
5	Rank	3	0	2.35	0.00	11.77	39.08
6	Clearance Level	3	60	2.35	141.25	78.74	38.90
7	Access Level	0	0	1.35	0.00	21.84	22.67
8	Previous Violations	0	5	1.36	6.80	22.13	22.55
9	Education Level	5	0	5.34	0.00	26.71	89.41
11	Characteristics of IT Components		30	0.21	6.36	4.24	3.51
12	Machine Type	3	20	2.36	47.14	20.70	33.41
13	Application	3	10	2.36	23.59	14.70	33.66
14	Connection Type	2	5	2.02	10.08	25.31	28.55
15	Authentication Type	1	10	1.69	16.92	23.32	24.03
16	Network	2	20	2.01	40.23	25.32	28.70
17	QoP/Encryption Level	3	30	2.38	71.32	97.02	33.62
18	Distance from requester to source	2	5	2.03	10.17	10.04	28.90
20	Heuristics		5	0.20	1.00	1.77	3.37
21	Risk Knowledge	2	50	1.99	99.60	101.61	101.22
22	Trust Level	2	50	2.01	100.32	100.67	100.88
24	Situational Factors		15	0.57	8.61	7.18	9.58
25	Specific Mission Role	1	30	1.67	50.07	46.38	33.85
26	Time Sensitivity of Information	8	25	8.34	208.38	156.53	166.87
27	Transaction Type	8	20	8.36	167.19	114.85	166.97
28	Auditable or Non-auditable	8	10	8.35	83.50	146.02	167.01
29	Audience Size	2	15	2.00	29.99	45.13	40.14
31	Environmental Factors		10	0.37	3.70	6.45	6.14
32	Current Location	2	80	2.04	162.96	115.85	101.21
33	Operational Environment Threat Level	5	20	5.36	107.14	227.75	267.34
35	Characteristics of Information Requested		10	0.59	5.88	8.83	9.80
36	Classification Level	2	10	2.03	20.27	78.54	40.17
37	Encryption Level	7	10	8.01	80.07	100.28	160.20
38	Network Classification Level	3	30	2.35	70.41	32.50	47.15
39	Permission Level	8	20	8.36	167.27	156.34	166.97
40	Perishable/Non-Perishable	9	30	8.67	260.24	141.20	173.59

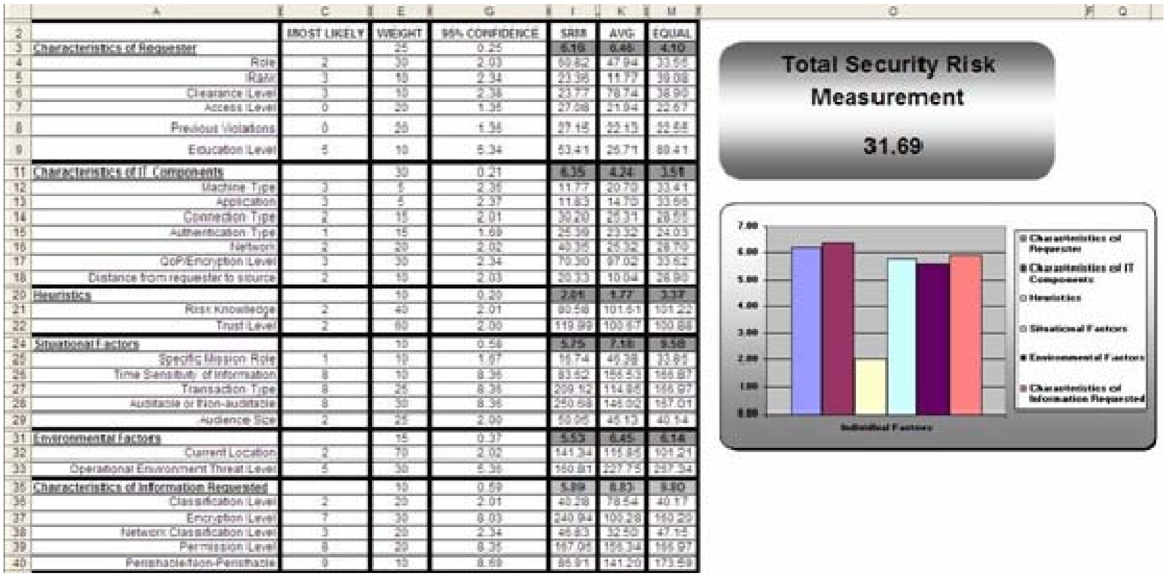
Total Security Risk Measurement

32.95

Table 7. Low Risk Scenario Physical Security Expert Results

c. Business Expert

The Business weightings scored the lowest of all the low risk at 31.69. The highest weighted risk category, Characteristics of IT Components, was almost a third greater than the average score 6.35 vs. 4.24. The Characteristics of Information Requested category was significantly lower than the average because of the 10% weighting assigned.



	A	C	E	G	I	K	M
2		MOST LIKELY	WEIGHT	95% CONFIDENCE	SRM	AVG	EQUAL
3	Characteristics of Requester		25	0.25	6.16	6.46	4.10
4	Role	2	30	2.03	60.82	47.94	33.55
5	Rank	3	10	2.34	23.36	11.77	39.08
6	Clearance Level	3	10	2.38	23.77	78.74	38.90
7	Access Level	0	20	1.35	27.08	21.84	22.67
8	Previous Violations	0	20	1.36	27.15	22.13	22.55
9	Education Level	5	10	5.34	53.41	26.71	89.41
11	Characteristics of IT Components		30	0.21	6.35	4.24	3.51
12	Machine Type	3	5	2.35	11.77	20.70	33.41
13	Application	3	5	2.37	11.83	14.70	33.66
14	Connection Type	2	15	2.01	30.20	25.31	28.55
15	Authentication Type	1	15	1.69	25.39	23.32	24.03
16	Network	2	20	2.02	40.35	25.32	28.70
17	QoP/Encryption Level	3	30	2.34	70.30	97.02	33.62
18	Distance from requester to source	2	10	2.03	20.33	10.04	28.90
20	Heuristics		10	0.20	2.01	1.77	3.37
21	Risk Knowledge	2	40	2.01	80.58	101.61	101.22
22	Trust Level	2	60	2.00	119.99	100.67	100.88
24	Situational Factors		10	0.58	5.75	7.18	9.58
25	Specific Mission Role	1	10	1.67	16.74	46.38	33.85
26	Time Sensitivity of Information	8	10	8.36	83.62	156.53	166.87
27	Transaction Type	8	25	8.36	209.12	114.85	166.97
28	Auditable or Non-auditable	8	30	8.36	250.68	146.02	167.01
29	Audience Size	2	25	2.00	50.05	45.13	40.14
31	Environmental Factors		15	0.37	5.53	6.45	6.14
32	Current Location	2	70	2.02	141.34	115.85	101.21
33	Operational Environment Threat Level	5	30	5.36	160.81	227.75	267.34
35	Characteristics of Information Requested		10	0.59	5.89	8.83	9.80
36	Classification Level	2	20	2.01	40.28	78.54	40.17
37	Encryption Level	7	30	8.03	240.94	100.28	160.20
38	Network Classification Level	3	20	2.34	46.83	32.50	47.15
39	Permission Level	8	20	8.35	167.05	156.34	166.97
40	Perishable/Non-Perishable	9	10	8.69	86.91	141.20	173.59

Total Security Risk Measurement

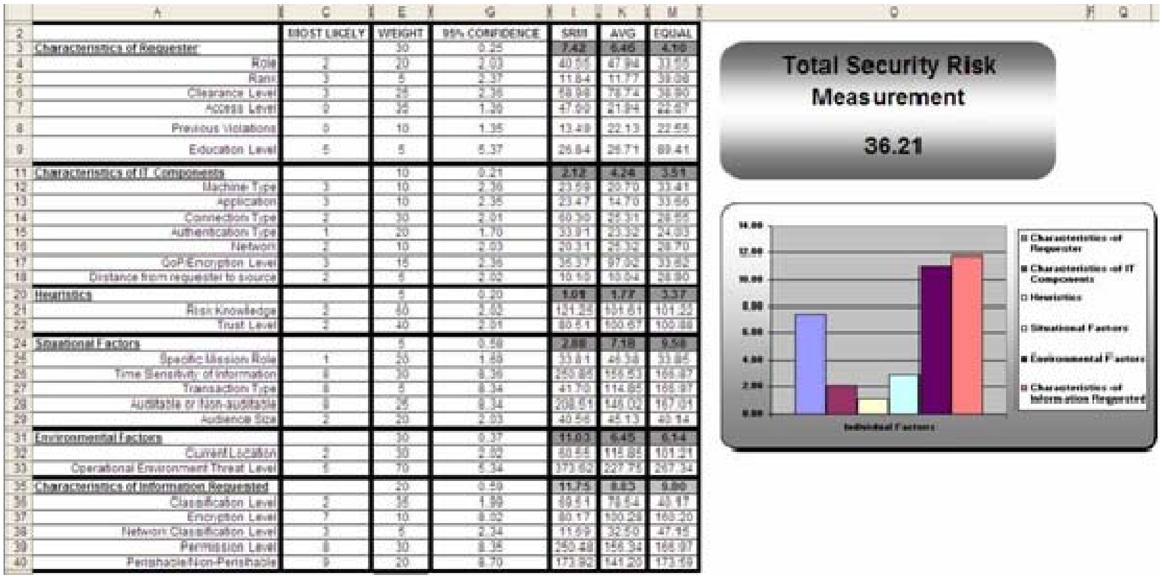
31.69

7.00
6.00
5.00
4.00
3.00
2.00
1.00
0.00
Individual Factors
Characteristics of Requester
Characteristics of IT Components
Heuristics
Situational Factors
Environmental Factors
Characteristics of Information Requested

Table 8. Low Risk Scenario Business Expert Results

d. *Information Assurance Expert*

The Information Assurance weightings came in second highest just above the average of 34.94 at 36.21. Due to the low emphasis on the Situational Factors, 5%, the results for this category were well below average. The Characteristics of Information Requested category was driven by the high risk involved with the information being perishable as well as the permissions granted. Even though the operational environment presented a medium threat, the emphasis placed on it caused the Environmental Factors to be almost double the average.



		MOST LIKELY	WEIGHT	95% CONFIDENCE	SRM	AVG	EQUAL
3	Characteristics of Requester		30	0.25	7.42	6.46	4.10
4	Role	2	20	2.03	40.55	47.94	33.55
5	Rank	3	5	2.37	11.84	11.77	39.08
6	Clearance Level	3	25	2.36	58.98	78.74	38.90
7	Access Level	0	35	1.30	47.90	21.94	22.47
8	Previous Violations	0	10	1.35	13.48	22.13	22.55
9	Education Level	5	5	5.37	26.84	26.71	89.41
11	Characteristics of IT Components		10	0.21	2.12	4.24	3.51
12	Machine Type	3	10	2.36	23.59	20.70	33.41
13	Application	3	10	2.35	23.47	14.70	33.56
14	Connection Type	2	30	2.01	60.30	25.31	28.55
15	Authentication Type	1	20	1.70	33.91	23.32	24.03
16	Network	2	10	2.03	20.31	25.32	28.70
17	CoP/Encryption Level	3	15	2.36	35.37	97.02	33.62
18	Distance from requester to source	2	5	2.02	10.10	10.04	28.80
20	Heuristics		5	0.20	1.01	1.77	3.37
21	Risk Knowledge	2	50	2.02	121.25	101.61	101.22
22	Trust Level	2	40	2.01	80.51	100.67	100.88
24	Situational Factors		5	0.58	2.88	7.18	9.58
25	Specific Mission Role	1	20	1.69	33.81	46.38	33.85
26	Time Sensitivity of Information	8	30	8.36	250.85	155.53	166.87
27	Transaction Type	8	5	8.34	41.70	114.85	166.87
28	Auditable or Non-auditable	8	25	8.34	208.51	146.02	167.01
29	Audience Size	2	20	2.03	40.56	45.13	40.14
31	Environmental Factors		30	0.37	11.03	6.45	6.14
32	Current Location	2	30	2.02	60.55	115.85	101.21
33	Operational Environment Threat Level	5	70	5.34	373.62	227.75	267.34
35	Characteristics of Information Requested		20	0.59	11.75	8.83	9.80
36	Classification Level	2	35	1.99	69.51	78.54	45.17
37	Encryption Level	7	10	8.02	80.17	100.28	160.20
38	Network Classification Level	3	5	2.34	11.69	32.50	47.15
39	Permission Level	8	30	8.35	250.48	156.34	166.97
40	Perishable/Non-Perishable	9	20	8.70	173.92	141.20	173.59

Total Security Risk Measurement

36.21

Table 9. Low Risk Scenario Information Assurance Expert Results

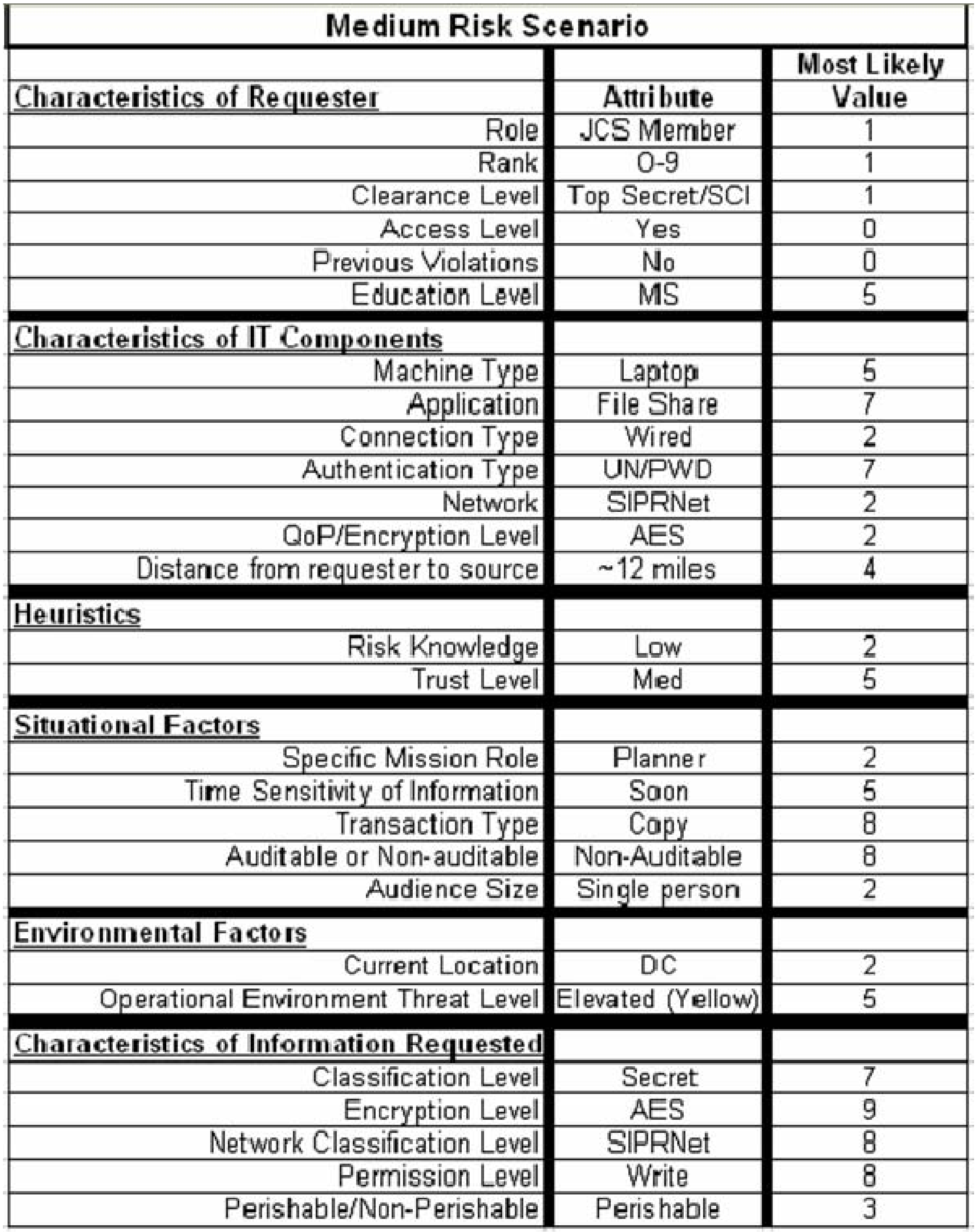
D. MEDIUM RISK SCENARIO, TESTS AND OBSERVATIONS

1. Medium Risk Test Scenario

A member of the Joint Chiefs is working on a new campaign plan for an operation in Afghanistan. He is working in a secure facility at the White House and needs Secret information located in a secure facility in Virginia. The Vice Admiral holds a Top Secret/SCI clearance with no previous security violations. He will be using a wired connection to his laptop to access information over the SIPRNet. The Admiral has permission to write to the file being requested. The situation is moderately time sensitive and the information being requested is perishable.

2. Medium Risk Most Likely Value Input

These numbers have been chosen arbitrarily throughout the scenario. They are based strictly on what we feel would be an appropriate risk value. Further research is needed to generate accurate inputs for this model. These numbers represent the most likely value in the triangle distribution portion of the TSRM model for the medium risk scenario.



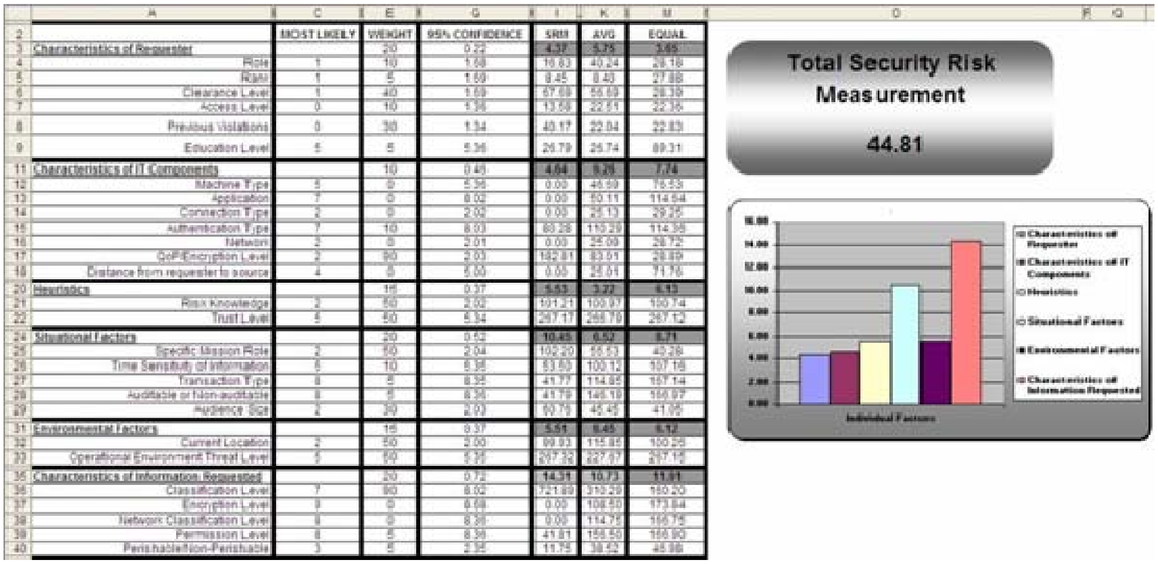
Medium Risk Scenario		
		Most Likely
Characteristics of Requester	Attribute	Value
Role	JCS Member	1
Rank	O-9	1
Clearance Level	Top Secret/SCI	1
Access Level	Yes	0
Previous Violations	No	0
Education Level	MS	5
Characteristics of IT Components		
Machine Type	Laptop	5
Application	File Share	7
Connection Type	Wired	2
Authentication Type	UN/PWD	7
Network	SIPRNet	2
QoP/Encryption Level	AES	2
Distance from requester to source	~12 miles	4
Heuristics		
Risk Knowledge	Low	2
Trust Level	Med	5
Situational Factors		
Specific Mission Role	Planner	2
Time Sensitivity of Information	Soon	5
Transaction Type	Copy	8
Auditable or Non-auditable	Non-Auditable	8
Audience Size	Single person	2
Environmental Factors		
Current Location	DC	2
Operational Environment Threat Level	Elevated (Yellow)	5
Characteristics of Information Requested		
Classification Level	Secret	7
Encryption Level	AES	9
Network Classification Level	SIPRNet	8
Permission Level	Write	8
Perishable/Non-Perishable	Perishable	3

Table 10. Medium Risk Scenario Most Likely Values

3. Medium Risk Test Results

a. Computer Science Expert

The Computer Science weighting returned the highest overall TSRM at 44.81. The Characteristics of IT Components category was well below average due to the emphasis placed on encryption level and the low most likely value for that factor. The Characteristics of Information Requested category was well above the average because of the high emphasis placed on classification level with a weight of 90%. With a most likely value of seven this factor drove the value significantly above average.



	A	C	E	G	I	K	M
2		MOST LIKELY	WEIGHT	95% CONFIDENCE	SRM	AVG	EQUAL
3	Characteristics of Requester		20	0.22	4.37	5.75	3.65
4	Role	1	10	1.69	16.83	40.24	28.18
5	Rank	1	5	1.69	8.45	8.40	27.88
6	Clearance Level	1	40	1.69	67.69	56.69	28.39
7	Access Level	0	10	1.36	13.58	22.51	22.36
8	Previous Violations	0	30	1.34	40.17	22.04	22.83
9	Education Level	5	5	5.36	26.79	25.74	89.31
11	Characteristics of IT Components		10	0.46	4.64	5.26	7.74
12	Machine Type	5	0	5.36	0.00	46.59	76.53
13	Application	7	0	8.02	0.00	50.11	114.54
14	Connection Type	2	0	2.02	0.00	25.13	29.25
15	Authentication Type	7	10	8.03	80.28	110.29	114.35
16	Network	2	0	2.01	0.00	25.09	28.72
17	QoP/Encryption Level	2	90	2.03	182.81	83.51	28.89
18	Distance from requester to source	4	0	5.00	0.00	25.01	71.76
20	Heuristics		15	0.37	5.53	3.22	6.93
21	Risk Knowledge	2	50	2.02	101.21	100.97	100.74
22	Trust Level	5	50	5.34	267.17	266.79	267.12
24	Situational Factors		20	0.52	10.45	6.52	8.71
25	Specific Mission Role	2	50	2.04	102.20	55.53	40.28
26	Time Sensitivity of Information	6	10	8.36	83.60	100.12	107.16
27	Transaction Type	8	5	8.35	41.77	114.85	167.14
28	Auditable or Non-auditable	8	5	8.36	41.79	146.19	166.97
29	Audience Size	2	30	2.03	60.79	45.45	41.05
31	Environmental Factors		15	0.37	5.51	6.45	6.12
32	Current Location	2	50	2.00	99.93	115.85	100.25
33	Operational Environment Threat Level	5	50	5.35	267.32	227.97	267.15
35	Characteristics of Information Requested		20	0.72	14.31	10.73	11.81
36	Classification Level	7	90	8.02	721.89	310.29	160.20
37	Encryption Level	9	0	8.68	0.00	108.50	173.64
38	Network Classification Level	8	0	8.36	0.00	114.75	166.75
39	Permission Level	8	5	8.36	41.81	156.50	166.90
40	Perishable/Non-Perishable	3	5	2.35	11.75	38.52	46.98

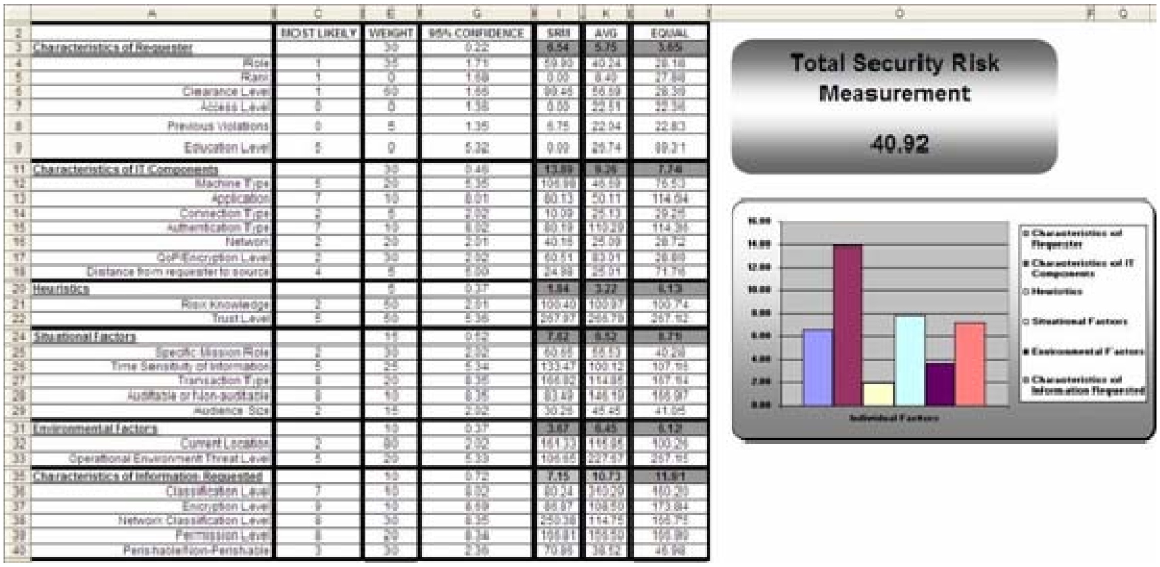
Total Security Risk Measurement

44.81

Table 11. Medium Risk Scenario Computer Science Expert Results

b. Physical Security Expert

The Physical Security weightings provided the lowest TSRM at 40.92. This was only slightly lower than the Business and Information Assurance results. The Characteristics of IT Components was higher than average because of the value from machine type and the overall weighting of 30% put on this category. The Characteristics of Information Requested category was lower than average despite the high risk and weight of the network classification because the overall weighting was only 10%. The Heuristics category was well below the average because of the low 5% weighting assigned to that category.



	A	C	E	G	I	K	M
2		MOST LIKELY	WEIGHT	95% CONFIDENCE	SRM	AVG	EQUAL
3	Characteristics of Requester		30	0.22	6.54	5.75	3.65
4	Role	1	35	1.71	59.90	40.24	28.18
5	Rank	1	0	1.68	0.00	8.40	27.88
6	Clearance Level	1	60	1.66	99.46	56.59	28.39
7	Access Level	0	0	1.38	0.00	22.51	22.36
8	Previous Violations	0	5	1.35	6.75	22.04	22.83
9	Education Level	5	0	5.32	0.00	26.74	89.21
11	Characteristics of IT Components		30	0.46	13.89	9.26	7.74
12	Machine Type	5	20	5.35	106.98	46.59	76.53
13	Application	7	10	8.01	80.13	50.11	114.64
14	Connection Type	2	5	2.02	10.09	25.13	29.25
15	Authentication Type	7	10	8.02	80.19	110.29	114.36
16	Network	2	20	2.01	40.15	25.09	28.72
17	QoP/Encryption Level	2	30	2.02	60.51	83.01	28.89
18	Distance from requester to source	4	5	5.00	24.98	25.01	71.76
20	Heuristics		5	0.37	1.84	3.27	6.13
21	Risk Knowledge	2	50	2.01	100.40	100.97	100.74
22	Trust Level	5	50	5.36	267.97	266.79	267.12
24	Situational Factors		11	0.52	7.82	6.52	6.71
25	Specific Mission Role	2	30	2.02	60.65	55.53	40.28
26	Time Sensitivity of Information	5	25	5.34	133.47	100.12	107.15
27	Transaction Type	8	20	8.35	166.92	114.85	167.14
28	Auditable or Non-auditable	8	10	8.35	83.49	146.19	166.97
29	Audience Size	2	15	2.02	30.26	45.45	41.05
31	Environmental Factors		10	0.37	3.67	6.45	6.12
32	Current Location	2	80	2.02	161.33	115.85	100.25
33	Operational Environment Threat Level	5	20	5.33	106.65	227.67	267.15
35	Characteristics of Information Requested		10	0.72	7.15	10.73	11.91
36	Classification Level	7	10	8.02	80.24	310.29	160.20
37	Encryption Level	9	10	8.69	86.87	108.50	173.84
38	Network Classification Level	8	30	8.35	250.38	114.75	166.75
39	Permission Level	8	20	8.34	166.81	155.50	166.90
40	Perishable/Non-Perishable	3	30	2.36	70.86	38.52	46.98

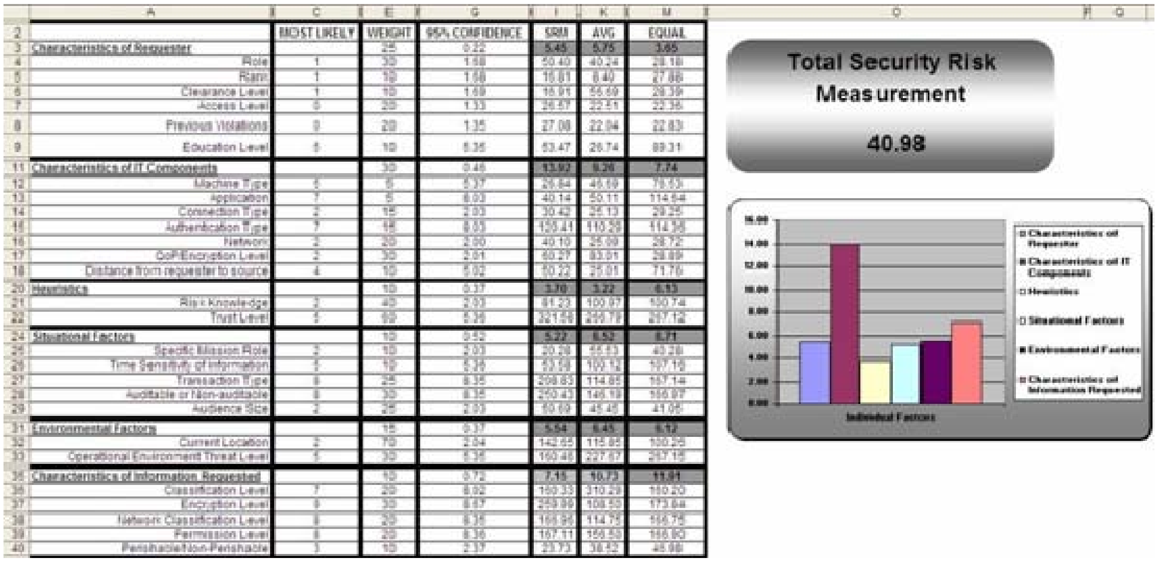
Total Security Risk Measurement

40.92

Table 12. Medium Risk Scenario Physical Security Expert Results

c. Business Expert

The Business weighting results provided a TSRM of 40.98. This score was the exact same score of the Information Assurance expert even though the distribution was quite different. The Characteristics of IT Components category was relatively high because of the high weighting value of 30%. This produced a risk much higher than the average. The Characteristics of Information Requested category was lower than the average because of the low weighting of 10%. In the Situational Factors category a large emphasis placed on transaction type and audit ability caused high results, but these were tempered by the category's overall low emphasis of 10%.



	A	C	E	G	I	K	M
2		MOST LIKELY	WEIGHT	95% CONFIDENCE	SRM	AVG	EQUAL
3	Characteristics of Requester		25	0.22	5.45	5.75	3.65
4	Role	1	30	1.68	50.40	40.24	28.18
5	Rank	1	10	1.58	15.81	8.40	27.88
6	Clearance Level	1	10	1.69	16.91	56.59	28.39
7	Access Level	0	20	1.33	26.57	22.51	22.36
8	Previous Violations	0	20	1.35	27.08	22.04	22.83
9	Education Level	5	10	5.35	53.47	26.74	89.31
11	Characteristics of IT Components		30	0.46	13.92	9.26	7.74
12	Machine Type	5	5	5.37	26.84	46.59	76.53
13	Application	7	5	8.03	40.14	50.11	114.64
14	Connection Type	2	15	2.03	30.42	25.13	29.25
15	Authentication Type	7	15	8.03	120.41	110.29	114.36
16	Network	2	20	2.00	40.10	25.09	28.72
17	QoP/Encryption Level	2	30	2.01	60.27	83.01	28.89
18	Distance from requester to source	4	10	5.02	50.22	25.01	71.76
20	Heuristics		10	0.37	3.70	3.22	6.13
21	Risk Knowledge	2	40	2.03	81.23	100.97	100.74
22	Trust Level	5	60	5.36	321.58	266.79	267.12
24	Situational Factors		10	0.52	5.22	6.52	6.71
25	Specific Mission Role	2	10	2.03	20.28	55.53	40.28
26	Time Sensitivity of Information	5	10	5.36	53.59	100.12	107.15
27	Transaction Type	8	25	8.35	208.83	114.85	167.14
28	Auditable or Non-auditable	8	30	8.35	250.43	146.19	166.97
29	Audience Size	2	25	2.03	50.69	45.45	41.05
31	Environmental Factors		15	0.37	5.54	6.45	6.12
32	Current Location	2	70	2.04	142.65	115.85	100.25
33	Operational Environment Threat Level	5	30	5.35	160.46	227.67	267.15
35	Characteristics of Information Requested		10	0.72	7.15	10.73	11.91
36	Classification Level	7	20	8.02	160.33	310.29	160.20
37	Encryption Level	9	30	8.67	259.99	108.50	173.84
38	Network Classification Level	8	20	8.35	166.96	114.75	166.75
39	Permission Level	8	20	8.36	167.11	155.50	166.90
40	Perishable/Non-Perishable	3	10	2.37	23.73	38.52	46.98

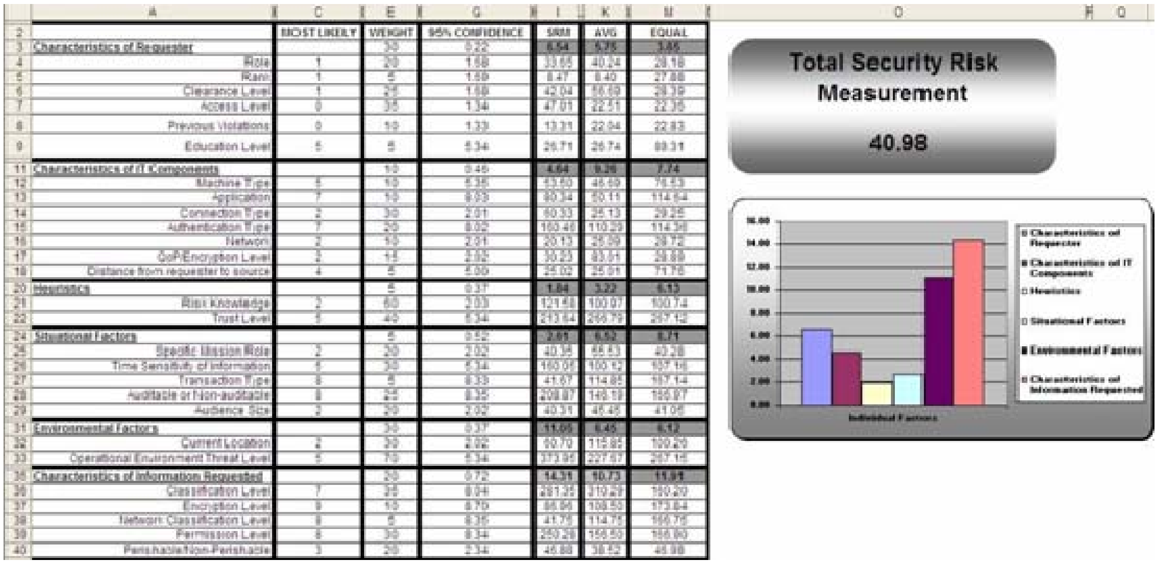
Total Security Risk Measurement

40.98

Table 13. Medium Risk Scenario Business Expert Results

d. *Information Assurance Expert*

The Information Assurance weighting results provided a TSRM of 40.98. This TSRM resulted in the same measure as the Business expert even though the weightings were different. The Situational Factors category was less than half of the average because of a low priority of only 5%. The Environmental Factors category was nearly double the average due to the heavy emphasis of 30% even though the most likely values were set at medium risks. The Characteristics of IT Components was half the average, once again, because of the low weighting of only 10% assigned to this category.



	A	C	E	G	I	K	M
2		MOST LIKELY	WEIGHT	95% CONFIDENCE	SRM	AVG	EQUAL
3	Characteristics of Requester		30	0.22	6.54	5.75	3.65
4	Role	1	20	1.58	33.65	40.24	28.18
5	Rank	1	5	1.59	8.47	8.40	27.88
6	Clearance Level	1	25	1.58	42.04	56.69	28.39
7	Access Level	0	35	1.34	47.01	22.51	22.35
8	Previous Violations	0	10	1.33	13.31	22.04	22.83
9	Education Level	5	5	5.34	26.71	26.74	89.31
11	Characteristics of IT Components		10	0.46	4.64	9.26	7.74
12	Machine Type	5	10	5.35	53.50	46.59	76.53
13	Application	7	10	8.03	80.34	50.11	114.64
14	Connection Type	2	30	2.01	60.33	25.13	29.25
15	Authentication Type	7	20	8.02	160.46	110.29	114.36
16	Network	2	10	2.01	20.13	25.09	28.72
17	GoP/Encryption Level	2	15	2.02	30.23	83.51	28.89
18	Distance from requester to source	4	5	5.00	25.02	25.01	71.76
20	Heuristics		5	0.37	1.84	3.22	6.13
21	Risk Knowledge	2	60	2.03	121.58	100.07	100.74
22	Trust Level	5	40	5.34	213.64	266.79	267.12
24	Situational Factors		5	0.52	2.61	6.52	8.71
25	Specific Mission Role	2	20	2.02	40.35	55.63	40.28
26	Time Sensitivity of Information	5	30	5.34	160.05	100.12	107.16
27	Transaction Type	8	5	8.33	41.67	114.85	167.14
28	Auditable or Non-auditable	8	25	8.35	208.87	149.19	166.87
29	Audience Size	2	20	2.02	40.31	45.45	41.05
31	Environmental Factors		30	0.37	11.05	6.45	6.12
32	Current Location	2	30	2.02	60.70	115.85	100.20
33	Operational Environment Threat Level	5	70	5.34	373.95	227.57	267.15
35	Characteristics of Information Requested		20	0.72	14.31	10.73	11.91
36	Classification Level	7	35	8.04	281.35	219.29	160.20
37	Encryption Level	9	10	8.70	86.96	108.50	173.64
38	Network Classification Level	8	5	8.35	41.75	114.75	166.75
39	Permission Level	8	30	8.34	250.28	156.50	166.80
40	Perishable/Non-Perishable	3	20	2.34	46.88	38.52	46.88

Total Security Risk Measurement

40.98

Table 14. Medium Risk Scenario Information Assurance Expert Results

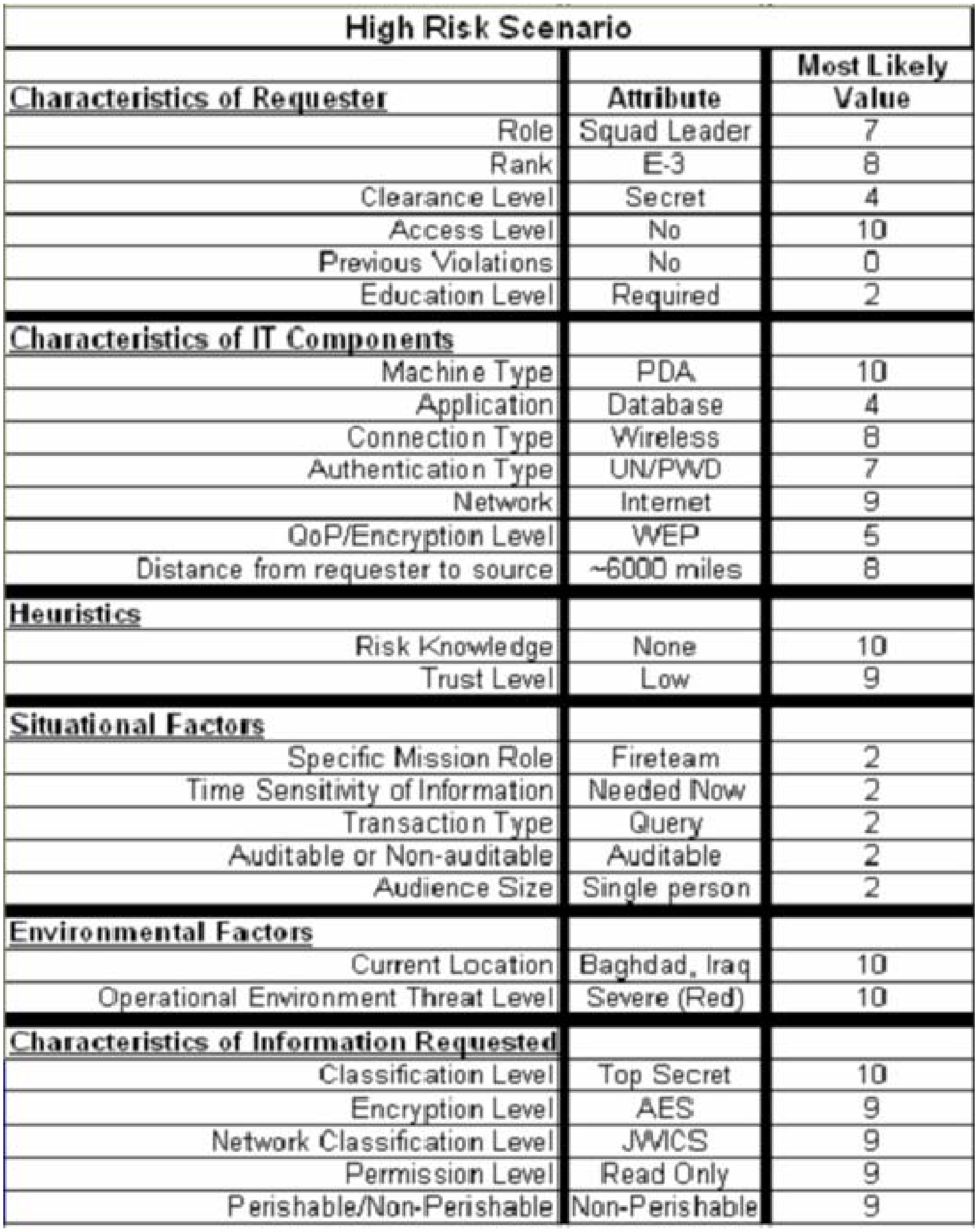
E. HIGH RISK SCENARIO, TESTS AND OBSERVATIONS

1. High Risk Test Scenario

A Marine Corp PFC is conducting house to house searches in Baghdad. He comes across someone who is believed to be a wanted terrorist. The name is not in his local database so he wants to query the CIA's database located in Virginia. The Marine holds a Secret clearance with no previous security violations and is requesting Top Secret information. The transaction is highly time sensitive and auditable. The information being requested is read-only and non-perishable.

2. High Risk Most Likely Value Input

These numbers have been chosen arbitrarily throughout the scenario. They are based strictly on what we feel would be an appropriate risk value. Further research is needed to generate accurate inputs for this model. These numbers represent the most likely value in the triangle distribution portion of the TSRM model for the high risk scenario.



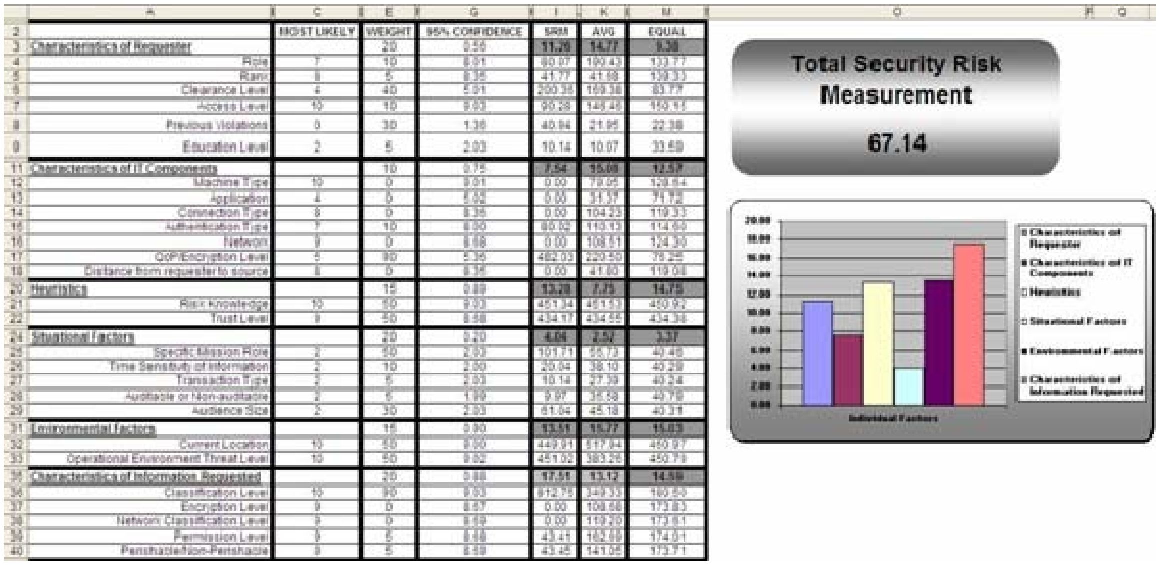
High Risk Scenario		
		Most Likely
Characteristics of Requester	Attribute	Value
Role	Squad Leader	7
Rank	E-3	8
Clearance Level	Secret	4
Access Level	No	10
Previous Violations	No	0
Education Level	Required	2
Characteristics of IT Components		
Machine Type	PDA	10
Application	Database	4
Connection Type	Wireless	8
Authentication Type	UN/PWD	7
Network	Internet	9
QoP/Encryption Level	WEP	5
Distance from requester to source	~6000 miles	8
Heuristics		
Risk Knowledge	None	10
Trust Level	Low	9
Situational Factors		
Specific Mission Role	Fireteam	2
Time Sensitivity of Information	Needed Now	2
Transaction Type	Query	2
Auditable or Non-auditable	Auditable	2
Audience Size	Single person	2
Environmental Factors		
Current Location	Baghdad, Iraq	10
Operational Environment Threat Level	Severe (Red)	10
Characteristics of Information Requested		
Classification Level	Top Secret	10
Encryption Level	AES	9
Network Classification Level	JWICS	9
Permission Level	Read Only	9
Perishable/Non-Perishable	Non-Perishable	9

Table 15. High Risk Scenario Most Likely Values

3. High Risk Test Results

a. Computer Science Expert

The Computer Science weighting results produced a TSRM of 67.14. This result was the second lowest and was below the average of 69.02. The Characteristics of IT Components category was about half the average because of the low weighting of 10% assigned. Heuristics was well above the average because of the relatively high emphasis of 15% assigned. This was the highest weighting of all the experts. The Characteristics of Information Requested category was driven higher than the average because of heavy weighting of 90% on the classification level and the high most likely value of ten assigned to that factor.



	A	C	E	G	I	K	M
2		MOST LIKELY	WEIGHT	95% CONFIDENCE	SRM	AVG	EQUAL
3	Characteristics of Requester		20	0.56	11.26	14.77	9.38
4	Role	7	10	8.01	80.07	190.43	133.77
5	Rank	8	5	8.35	41.77	41.88	139.33
6	Clearance Level	4	40	5.01	200.38	169.38	83.77
7	Access Level	10	10	9.03	90.28	145.46	150.55
8	Previous Violations	0	30	1.36	40.84	21.95	22.38
9	Education Level	2	5	2.03	10.14	10.07	33.59
11	Characteristics of IT Components		10	0.75	7.54	15.08	12.57
12	Machine Type	10	0	9.01	0.00	79.05	128.64
13	Application	4	0	5.02	0.00	31.37	71.72
14	Connection Type	8	0	8.36	0.00	104.23	119.33
15	Authentication Type	7	10	8.00	80.02	110.13	114.60
16	Network	9	0	8.68	0.00	108.51	124.30
17	QoP/Encryption Level	5	90	5.36	482.03	220.50	76.25
18	Distance from requester to source	8	0	8.35	0.00	41.80	119.08
20	Heuristics		15	0.89	13.28	7.75	14.75
21	Risk Knowledge	10	50	9.03	451.34	451.53	450.92
22	Trust Level	9	50	8.68	434.17	434.55	434.38
24	Situational Factors		20	0.20	4.06	2.57	3.37
25	Specific Mission Role	2	50	2.03	101.71	55.73	40.45
26	Time Sensitivity of Information	2	10	2.00	20.04	38.10	40.29
27	Transaction Type	2	5	2.03	10.14	27.39	40.24
28	Auditable or Non-auditable	2	5	1.99	9.97	35.58	40.79
29	Audience Size	2	30	2.03	61.04	45.18	40.31
31	Environmental Factors		15	0.90	13.51	15.77	15.03
32	Current Location	10	50	9.00	449.91	517.94	450.97
33	Operational Environment Threat Level	10	50	9.02	451.02	383.26	450.79
35	Characteristics of Information Requested		20	0.88	17.51	13.12	14.59
36	Classification Level	10	90	9.03	812.75	349.33	180.50
37	Encryption Level	9	0	8.67	0.00	108.68	173.83
38	Network Classification Level	9	0	8.69	0.00	119.20	173.81
39	Permission Level	9	5	8.68	43.41	162.69	174.01
40	Perishable/Non-Perishable	9	5	8.69	43.45	141.05	173.71

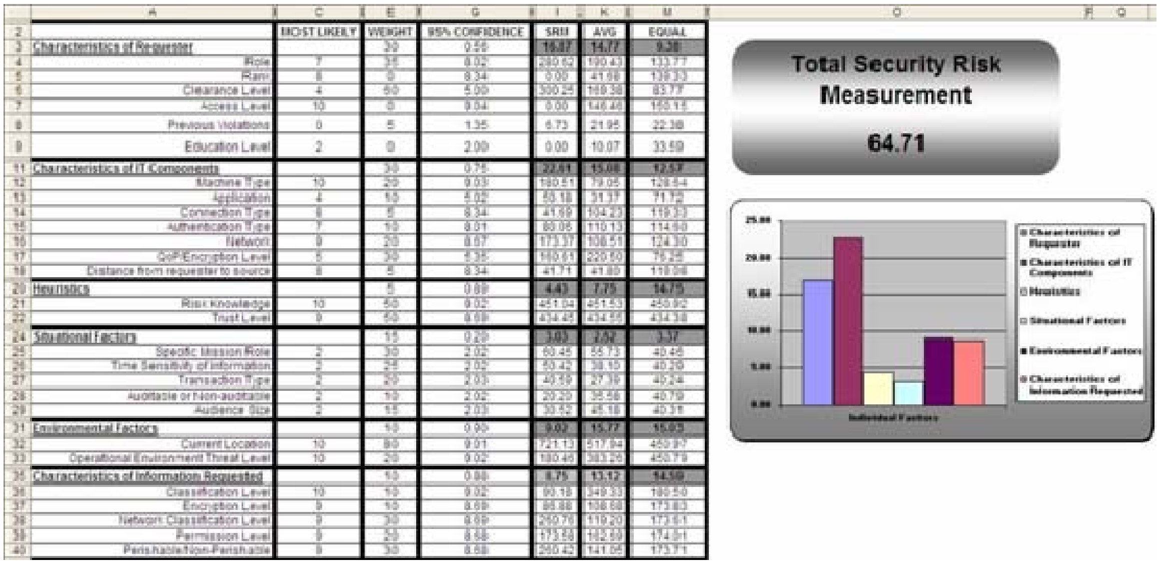
Total Security Risk Measurement

67.14

Table 16. High Risk Scenario Computer Science Expert Results

b. Physical Security Expert

The Physical Security weightings produced the lowest TSRM in the high risk category of 64.71. This result is nearly ten points lower than the high value of 74.46 obtained by the Information Assurance weightings. The Characteristics of IT Components was higher than the average because of the high weighting of 30%. The Machine type factor produced a value of twice the average because of a most likely value of ten and a weighting of 20%. The Connection type factor was less than half the average even though the most likely value was an eight because of a low weighting of 5%. The Characteristics of Information Requested category was well below average because of the low emphasis of 10% assigned. The Classification level factor weighting of 10% produced a risk that was significantly below the average even though the most likely value was a ten. The weighting of 30% assigned to the Network classification level produced a result of more than twice average.



	A	C	E	G	I	K	M
2		MOST LIKELY	WEIGHT	95% CONFIDENCE	SRM	AVG	EQUAL
3	Characteristics of Requester		30	0.58	16.87	14.77	9.28
4	Role	7	35	8.02	280.62	190.43	133.77
5	Rank	8	0	8.34	0.00	41.68	139.33
6	Clearance Level	4	60	5.00	300.25	169.38	83.77
7	Access Level	10	0	9.04	0.00	146.46	150.15
8	Previous Violations	0	5	1.35	6.73	21.95	22.38
9	Education Level	2	0	2.00	0.00	10.07	33.59
11	Characteristics of IT Components		30	0.75	22.61	15.08	12.57
12	Machine Type	10	20	9.03	180.51	79.05	128.54
13	Application	4	10	5.02	50.18	31.37	71.72
14	Connection Type	8	5	8.34	41.69	104.23	119.33
15	Authentication Type	7	10	8.01	80.06	110.13	114.60
16	Network	9	20	8.67	173.37	108.51	124.30
17	QoP/Encryption Level	5	30	5.35	160.61	220.50	76.25
18	Distance from requester to source	8	5	8.34	41.71	41.80	119.08
20	Heuristics		5	0.89	4.43	7.75	14.75
21	Risk Knowledge	10	50	9.02	451.04	451.53	450.92
22	Trust Level	9	50	8.69	434.45	434.55	434.38
24	Situational Factors		15	0.29	3.03	2.52	3.37
25	Specific Mission Role	2	30	2.02	60.45	55.73	40.45
26	Time Sensitivity of Information	2	25	2.02	50.42	38.10	40.20
27	Transaction Type	2	20	2.03	40.59	27.39	40.24
28	Auditable or Non-auditable	2	10	2.02	20.20	35.56	40.79
29	Audience Size	2	15	2.03	30.52	45.18	40.31
31	Environmental Factors		10	0.90	9.02	15.77	15.03
32	Current Location	10	80	9.01	721.13	517.94	450.87
33	Operational Environment Threat Level	10	20	9.02	180.46	383.26	450.79
35	Characteristics of Information Requested		10	0.88	8.75	13.12	14.59
36	Classification Level	10	10	9.02	90.18	349.33	180.50
37	Encryption Level	9	10	8.69	86.88	108.68	173.83
38	Network Classification Level	9	30	8.69	260.76	119.20	173.81
39	Permission Level	9	20	8.58	173.58	162.59	174.01
40	Perishable/Non-Perishable	9	30	8.68	260.42	141.05	173.71

Total Security Risk Measurement

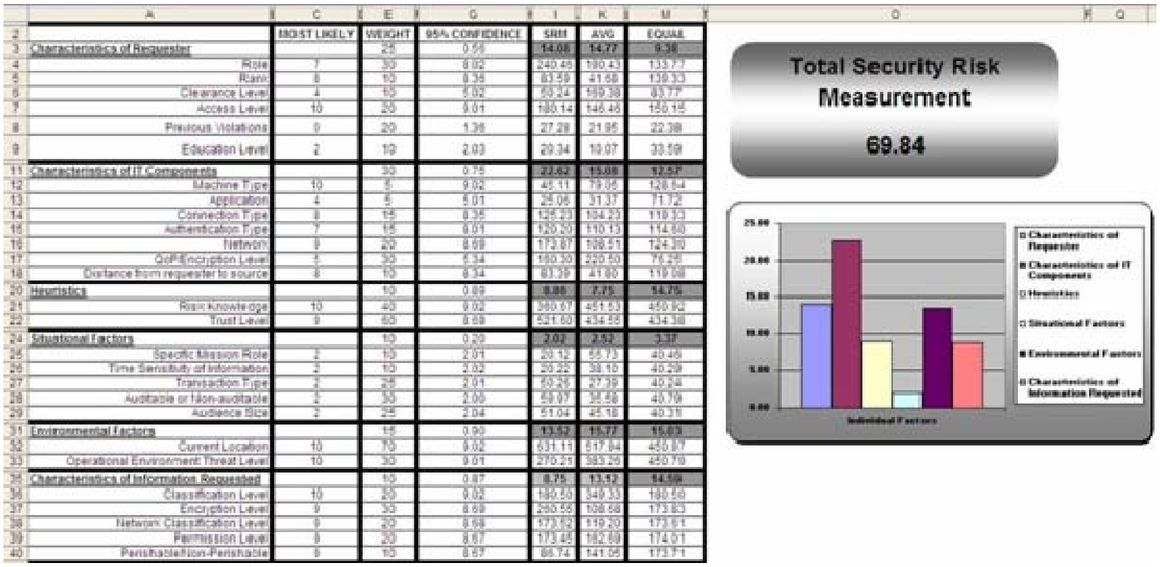
64.71

25.00
20.00
15.00
10.00
5.00
0.00
Individual Factors
Characteristics of Requester
Characteristics of IT Components
Heuristics
Situational Factors
Environmental Factors
Characteristics of Information Requested

Table 17. High Risk Scenario Physical Security Expert Results

c. Business Expert

The Business expert’s results were near average. A TSRM of 69.84 was only 0.82 higher than the average of 69.02. The Characteristics of IT Components category was one third above the average because of a heavy emphasis of 30% and a Network risk factor measurement well above the average. The Characteristics of Information Requested was below the average because of the low weighting of 10%. Within this category, the Encryption level factor was one and a half times greater than the average while the Classification level was nearly half the average.



	A	C	E	G	I	K	M
2		MOST LIKELY	WEIGHT	95% CONFIDENCE	SRM	AVG	EQUAL
3	Characteristics of Requester		25	0.56	14.06	14.77	9.38
4	Role	7	30	8.02	240.46	190.43	133.77
5	Rank	8	10	8.36	83.59	41.68	139.33
6	Clearance Level	4	10	5.02	50.24	159.38	83.77
7	Access Level	10	20	9.01	180.14	146.46	150.15
8	Previous Violations	0	20	1.36	27.28	21.95	22.38
9	Education Level	2	10	2.03	20.34	10.07	33.59
11	Characteristics of IT Components		30	0.75	22.62	15.08	12.57
12	Machine Type	10	5	9.02	45.11	79.06	128.64
13	Application	4	5	5.01	25.06	31.37	71.72
14	Connection Type	8	15	8.35	125.23	104.23	119.33
15	Authentication Type	7	15	8.01	120.20	110.13	114.60
16	Network	9	20	8.69	173.87	108.51	124.30
17	QoP/Encryption Level	5	30	5.34	160.30	220.50	76.25
18	Distance from requester to source	8	10	8.34	83.39	41.80	119.08
20	Heuristics		10	0.89	8.88	7.75	14.75
21	Risk Knowledge	10	40	9.02	360.67	451.53	450.92
22	Trust Level	9	60	8.69	521.60	434.55	434.38
24	Situational Factors		10	0.20	2.02	2.52	3.37
25	Specific Mission Role	2	10	2.01	20.12	55.73	40.46
26	Time Sensitivity of Information	2	10	2.02	20.22	38.10	40.29
27	Transaction Type	2	25	2.01	50.26	27.39	40.24
28	Auditable or Non-auditable	2	30	2.00	59.97	35.58	40.79
29	Audience Size	2	25	2.04	51.04	45.18	40.31
31	Environmental Factors		15	0.90	13.52	15.77	15.03
32	Current Location	10	70	9.02	631.11	617.84	450.87
33	Operational Environment Threat Level	10	30	9.01	270.21	383.26	450.78
35	Characteristics of Information Requested		10	0.87	8.75	13.12	14.50
36	Classification Level	10	20	9.02	180.50	349.33	180.50
37	Encryption Level	9	30	8.69	260.55	108.58	173.83
38	Network Classification Level	9	20	8.68	173.52	119.20	173.61
39	Permission Level	9	20	8.67	173.45	162.69	174.01
40	Perishable/Non-Perishable	9	10	8.67	86.74	141.06	173.71

Total Security Risk Measurement

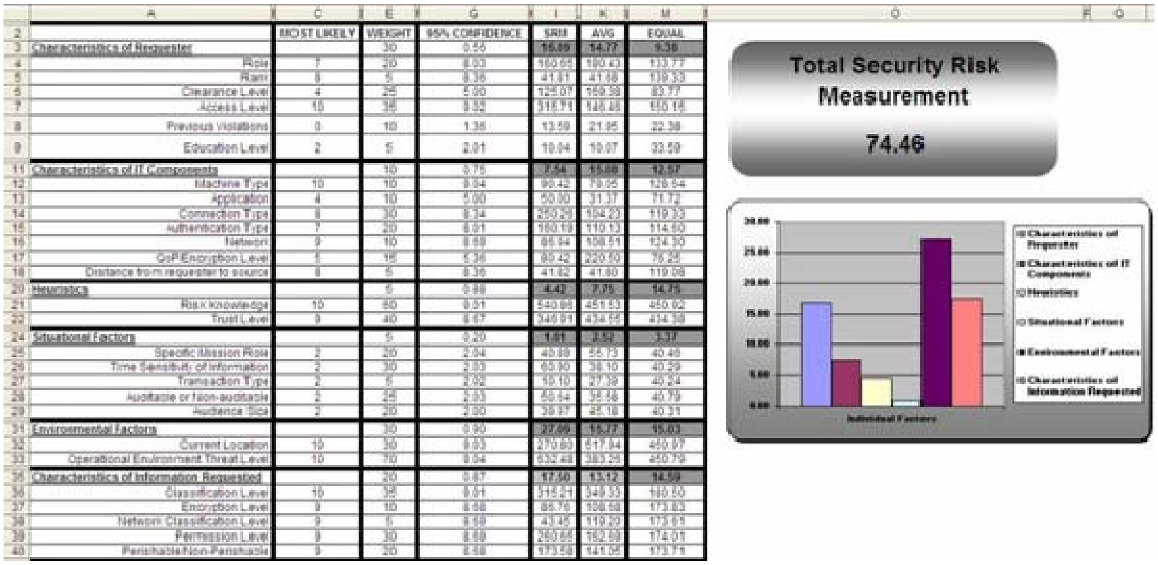
69.84

O
P
Q
25.00
20.00
15.00
10.00
5.00
0.00
Individual Factors
Characteristics of Requester
Characteristics of IT Components
Heuristics
Situational Factors
Environmental Factors
Characteristics of Information Requested

Table 18. High Risk Scenario Business Expert Results

d. *Information Assurance Expert*

The Information Assurance weightings provided the highest TSRM of 74.46. This result was well above the other results with nearly a ten point gap above the lowest TSRM in the High Risk Scenario. The Characteristics of IT Components category was only half the average because of the low weighting of 10%. The risk factor of Connection type was two and a half times the average due to the 30% weighting assigned. The Environmental Factors category was almost twice the average. With a weighting of 30%, the emphasis placed on this category was double that of the next closest expert's weighting. Within this category, the Operational environment factor was much higher than the average because of the 70% weighting assigned. The Characteristics of Information Requested category was about third higher than the average because of 20% weighting assigned to the category and also the 30% weighting assigned to the permission level.



	A	C	E	G	I	K	M
2		MOST LIKELY	WEIGHT	95% CONFIDENCE	SRM	AVG	EQUAL
3	Characteristics of Requester		30	0.56	16.89	14.77	9.36
4	Role	7	20	8.03	160.65	180.43	133.77
5	Rank	8	5	8.36	41.81	41.88	139.33
6	Clearance Level	4	25	5.00	125.07	169.38	83.77
7	Access Level	10	35	9.02	315.71	148.48	150.15
8	Previous Violations	0	10	1.36	13.59	21.95	22.38
9	Education Level	2	5	2.01	10.04	10.07	33.59
11	Characteristics of IT Components		10	0.75	7.54	15.88	12.57
12	Machine Type	10	10	9.04	90.42	79.05	128.54
13	Application	4	10	5.00	50.00	31.37	71.72
14	Connection Type	8	30	8.34	250.28	104.23	119.33
15	Authentication Type	7	20	8.01	160.19	110.13	114.60
16	Network	9	10	8.69	86.94	108.51	124.30
17	QoP Encryption Level	5	15	5.36	80.42	220.50	76.25
18	Distance from requester to source	8	5	8.36	41.82	41.80	119.08
20	Heuristics		5	0.88	4.42	7.75	14.75
21	Risk Knowledge	10	60	9.01	540.86	451.53	450.92
22	Trust Level	9	40	8.67	346.91	434.55	434.38
24	Situational Factors		5	0.20	1.01	2.52	3.37
25	Specific Mission Role	2	20	2.04	40.88	55.73	40.46
26	Time Sensitivity of Information	2	30	2.03	60.90	38.10	40.29
27	Transaction Type	2	5	2.02	10.10	27.39	40.24
28	Auditable or Non-auditable	2	25	2.03	50.64	35.58	40.79
29	Audience Size	2	20	2.00	39.97	45.18	40.31
31	Environmental Factors		30	0.90	27.09	15.77	15.03
32	Current Location	10	30	9.03	270.80	517.94	450.87
33	Operational Environment Threat Level	10	70	9.04	632.48	383.25	450.79
35	Characteristics of Information Requested		20	0.87	17.50	13.12	14.59
36	Classification Level	10	35	9.01	315.21	349.33	180.50
37	Encryption Level	9	10	8.68	86.76	108.68	173.83
38	Network Classification Level	9	5	8.69	43.45	119.20	173.65
39	Permission Level	9	30	8.69	260.66	162.69	174.01
40	Perishable/Non-Perishable	9	20	8.68	173.58	141.05	173.71

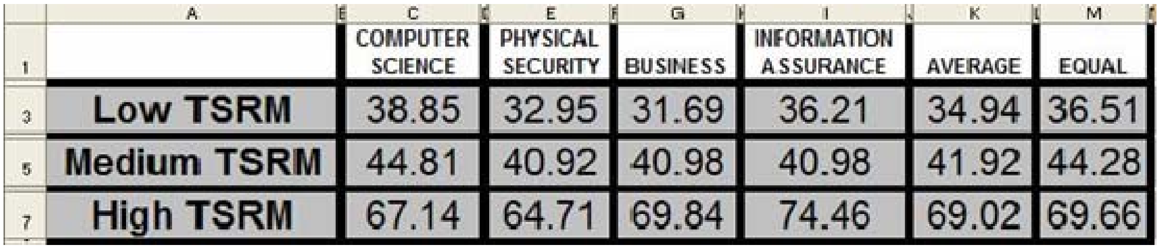
Total Security Risk Measurement

74.46

Table 19. High Risk Scenario Information Assurance Expert Results

F. RESULTS

Overall the TSRM model we created measures the risk for the given categories appropriately. The low risk scenario returns a lower value than the value returned for the medium and high risk scenarios. The medium scenario returned a TSRM value higher than the low risk scenario and lower than the high risk scenario. The high risk scenario returned values that were higher than both the low and medium risk scenarios.



	A	C	E	G	I	K	M
1		COMPUTER SCIENCE	PHYSICAL SECURITY	BUSINESS	INFORMATION ASSURANCE	AVERAGE	EQUAL
3	Low TSRM	38.85	32.95	31.69	36.21	34.94	36.51
5	Medium TSRM	44.81	40.92	40.98	40.98	41.92	44.28
7	High TSRM	67.14	64.71	69.84	74.46	69.02	69.66

Table 20. Summary of TSRM Results

Table 20 shows a summary of all the scenario results. The differences between the expert's weight sets and results were interesting. The low risk scenario had a range of just over seven points with three of the results falling below the equal weightings. The medium risk scenario ended up with three of the results within 6 hundredths of a percent, with two being exact, and one nearly four points higher than the rest. Once again, three of the results were below the equal weighting results. The high risk scenario had an almost ten point spread between the high and low TSRM. Only two of the results were below the equal weighting results and there were at least two points between each of the results.

These kinds of results show the effects that different weightings will have on the TSRM and this must be kept in mind when designing the RAdAC engine. The Computer Science expert produced the highest TSRM in both the low and medium risk scenarios while the Physical Security expert produced the lowest TSRM in both the medium and high risk scenarios. The Business expert had the lowest TSRM for the low risk scenario and the Information Assurance expert had the highest TSRM for the high risk scenario. Each of the experts had results that were either at the top or bottom of one of the scenarios with none of the results simply in the middle. This shows that each of the experts provided weightings that were significant in each of the scenarios and therefore none of the expert's results could be eliminated without affecting the overall results of this thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. RECOMMENDED FURTHER RESEARCH AND THESIS CONCLUSION

A. CHAPTER OVERVIEW

This chapter will provide a list of recommended future research topics for both the risk portion of the RAdAC engine and RAdAC as a whole. The discussion includes the main issues that were uncovered during research and several software programs that may be beneficial in building working models of the RAdAC engine and may be able to provide insight into what risk factors are the most important.

B. RECOMMENDED FURTHER TSRM MODULE RESEARCH

1. Delphi Method

We interviewed several experts in a variety of fields to get their opinion on what risk factors were important and how they should be weighted. Due to time constraints, the number of experts polled in each field was limited. Each participant we interviewed provided valuable insight into the individual risk factors, the weighting of those factors and RAdAC in general. Given more time, multiple experts in each field should be polled. A possible consensus amongst each group of experts could then be reached through the Delphi Method and the weight sets would be assigned in this manner (Mun, 2006). This method of assigning weight sets is a more robust and accepted manner on which to assign values if no historical data exists.

2. Risk Factor Analysis

We attempted to identify risk factors that we felt were most important when completing the Total Security Risk Measurement. However, a number of new issues were brought up when discussing our risk factors with experts. The identification of a more comprehensive list of risk factors is an essential next step, including direct and correlative risk factors. Taking that list and then narrowing down to those risks that are most important is one of the next steps in completing a working RAdAC engine.

3. Thesis Assumptions

Each of our assumptions needs to be researched further. These include:

a. Authentication

We did not account for any false positives for authentication. We assumed the transaction initiator (human or machine) is who he says he is. This included all components of the system used for initiation and transmission of the transaction.

b. System Failures

System failures including hardware and software failures were not addressed. We also did not account for the uncertainty associated with human or machine error.

c. Information Assurance

This thesis did not account for the risk involved with information integrity or availability. We assumed the information was available, accurate and was not compromised during transmission.

4. Actual Data Collection

The first major issue we encountered while doing this thesis was the lack of available data. An attempt was made to use bank transaction data and credit card transaction data to simulate information transaction statistics. The proprietary nature of much of the commercial banking data made it difficult to explore this area. Likely, any study done in this realm would have to be accomplished in the classified arena.

In order to accurately calculate the risk associated with a particular factor, data is needed. Once real world data is collected, it can be used in various probability distributions to calculate a much more accurate risk value.

Ways to collect, store and analyze data all need to be developed. One possibility we came across is the use of XML data tagging. A data set could be collected and then put into a working RAdAC model to determine actual risk measurements. Data tags could then be used to update a working RAdAC engine in real time.

5. Relationship of Individual Risk Factors

One of the major assumptions that we made in our research was the independence of the risk factors. That is to say, that no one risk factor impacted another risk factor. An actual working RAdAC engine would have several factors that are dynamically interdependent.

One example brought up in the expert opinion survey suggested that if a certain type of encryption is used, that the others factors in that category would be irrelevant because the encryption would protect the data. Another example mentioned was the comparison between the classification of the data and the clearance of the requester. If the data is classified lower than the clearance, this should change the weighting of these factors to lower the risk. If the data is classified higher than the clearance, this should change the weighting to greatly increase the risk. These types of relationships could mean that each transaction could dynamically change the risk factors that are being looked at and the weightings that are being applied.

The issue of risk factor dependency can be addressed by an influence net. Further headway toward a working RAdAC engine can be made by developing a Bayesian based model and determining the associations and weighting that each of the risk factors have upon one another.

6. Programs Evaluated

Throughout this research several software programs were investigated to assist in the calculation of risk. Each of these programs has characteristics that could make them useful in creating and validating a model of the RAdAC engine. These programs are briefly described below.

a. SIAM from SAIC

A Situational Influence Assessment Model (SIAM) can graphically depict factors in a belief net structure and then apply Bayesian probability techniques to assess the relationship among factors to determine the overall probability of occurrence. SIAM can also be used to determine critical pressure points, conduct what-if analysis as well as identify unintended consequences of specific actions. The original goal of the thesis was to use the SIAM program to model the RAdAC security risk measurement function. The various risk factors could be entered into SIAM as nodes and then different weights and link strengths could be applied to see how the top node, in this case the total risk, is affected. Due to time constraints we were unable to put our results into SIAM and build a model. This may still provide some beneficial results especially in identifying the relationships between the various factors (http://www.saic.com/products/software/siam/).

b. @Risk from Palisade

@Risk is a Microsoft Excel add-in that uses Monte Carlo simulation to show you many possible outcomes. It allows a user to replace uncertain values in a spreadsheet with probability distribution functions. @Risk can also provide a user with Sensitivity and Scenario Analyses to determine the critical factors in a model. This allows the user to rank the distribution functions in the model according to the impact they have on the output (http://www.palisade.com/risk/).

c. PrecisionTree from Palisade

PrecisionTree is a Decision Analysis add-in for Microsoft Excel. It is used to build decision trees and influence diagrams directly in a spreadsheet. The user can create diagrams easily by selecting cells in the spreadsheet and clicking node buttons at the PrecisionTree toolbar. Once a model is built, PrecisionTree will run a powerful decision analysis determining the best way to proceed. Using PrecisionTree lets the user detail all of the possible options and identify the best decision to make. Another possible useful option is PrecisionTree's Risk Profile feature. A decision analysis in PrecisionTree generates a Risk Profile. The Risk Profile compares the payoffs and risk of different decision options (http://www.palisade.com/precisiontree/).

d. Real Options from Decisioneering

Real Options is a Microsoft Excel add-in that uses a systematic approach and integrated solution using modeling in applying options theory in a dynamic and uncertain environment where decisions are flexible in the context of strategic decision-making. The Real Options approach incorporates a learning model, such that management makes better and more informed strategic decisions when some levels of uncertainty are resolved through the passage of time. Real Options uses a mix of Monte Carlo path-dependent simulation methods, closed-form solutions, partial differential equations, and binomial lattice trees (http://www.decisioneering.com/rotoolkit/).

C. RECOMMENDED FURTHER RESEARCH FOR RADAC

1. Policy for Weighting

Policies for setting the risk values and weighting will likely come down from higher authorities within DoD. As shown in this thesis through the expert opinions, there are great differences in what risk factors various groups deem important. Getting policy makers in the DoD to agree on which factors are important and how they should be weighted will be a difficult obstacle to the implementation of RAdAC. A process such as the Delphi Method, discussed above, could be useful with this problem also.

2. Units of Measure

The risk factors identified in this thesis vary from the characteristics of people, to IT equipment, to threat levels. These factors are not of equal magnitude or measure. It is unrealistic to weigh the risk of someone's rank against the risk of a network device on the same linear scale. Research is needed to develop various scales of measure that can adapt the different types of risk factors.

3. The Remainder of the RAdAC Engine

This thesis only addressed the security measurement of the RAdAC engine. There is still research needed on how to quantify the operational need and then how to make a final access decision. The three main functions of the RAdAC engine must be able to operate both independent of each other and as one unit. Developing models for each of the functions and then incorporating them into a single working model will provide a great step forward for the realization of RAdAC.

4. A Feedback Mechanism

In order for the RAdAC engine to dynamically adjust and for commanders to apply policies that maximize information flow, there needs to be a feedback loop. The feedback loop should capture how successful the information transaction was and how the information was used to improve a mission. The feedback loop also needs to be able to capture how a denied request affected a mission. Learning how the RAdAC decisions affect mission outcomes will provide a large step forward for the RAdAC engine. Another important piece of the feedback loop is related to the Trust Level risk factor. Research needs to be conducted on how best to capture both successful and unsuccessful transactions in a way that the results can be used to build trust within the system.

D. THESIS CONCLUSION

In summary, this thesis provided the requirements for RAdAC as part of the Global Information Grid and the NetOps construct. A brief overview was given on currently existing access control methods. Following the existing access control methods, the RAdAC concept was explained in detail.

Our research first yielded a list of possible RAdAC risk factors. These factors were grouped in the NSA identified risk categories; Characteristics of Requester, Characteristics of IT Components, Heuristics, Situational Factors, Environmental Factors and Characteristics of Information Requested. While the identified factors are not intended to be a complete list, it will provide a preliminary list of possible factors to be incorporated into a working RAdAC engine.

The next step in our thesis was to identify a process to quantify the risk associated with each factor. Without existing statistical data on the risk factors we decided to use a triangle distribution to simulate real world data. An Excel model was used to calculate a most likely value that accounts for uncertainty through Monte Carlo simulation. We assigned an initial arbitrary most likely value to each of the risk factors and ran the value through 5,000 iterations of the Monte Carlo simulation. The simulation returned a final most likely value with a 95% confidence level.

Following the identification of risk factors and the process of calculating values with uncertainty, a weighting scheme was needed in order to calculate the total risk. We interviewed experts in the fields of Business, Physical Security, Information Assurance and Computer Science. They provided us with their opinion on how the risk factors should be weighted. We formed an aggregate list, analyzed each of their results and compared and contrasted the results to the equal weight and average weighting baselines.

The final step of the thesis was to calculate the Total Security Risk Measurement. The calculated most likely value was multiplied by the expert weightings and the results were summed to provide the total risk. The model was tested for accuracy using several boundary case scenarios and the results were presented and explained.

Whether or not RAdAC as it is known today is successful, the process outlined in this thesis to calculate the TSRM can be utilized as the next generation of risk adaptable access control is formulated. As risk factors are identified and formalized in policy, statistics can be gathered to provide a useful near real time database which to run the RAdAC engine. Calculating the operational need, the final access decision and determining and managing the digital policies are just a few of the big pieces of the puzzle needed to get a working RAdAC engine. While an enormous amount of work still exists for RAdAC to come to fruition, this thesis provides some of the groundwork required to change from the need-to-know paradigm that exists today to the need-to-share environment required in the future.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Adams, William J., and Nathaniel J. Davis. Toward a Decentralized Trust-Based Access. IEEE Workshop on Information Assurance and Security, 16 June 2005, United States Military Academy, West Point, NY.

Choudhary, Abdur R. Compound Identity Measure: A New Concept for Information Assurance. IEEE Workshop on Information Assurance, 22 June 2006, United States Military Academy, West Point, NY.

Choudhary, Abdur R. Context-Based Adaptive Control in Autonomous Systems. IEEE Workshop on Information Assurance, 10 June 2004, United States Military Academy, West Point, NY.

Choudhary, Abdur R. A Policy Based Architecture for NSA RAdAC Model. IEEE Workshop on Information Assurance and Security, 16 June 2005, United States Military Academy, West Point, NY.

Choudhary, Abdur R. "Policy-Based Network Management." Bell Labs Technical Journal 9 (2004): 19-29.

CNSS Instruction No. 4009 National Information Assurance Glossary. Committee on National Security Systems. 2006.

Curphey, Mark. "Role Based Access Control." A Guide to Building Secure Web Applications. 22 Sept. 2002. The Open Web Application Security Project. 10 Nov. 2006 <http://www.cgisecurity.com/owasp/html/index.html>.

Denning, Dorothy E. Information Warfare and Security. New York: ACM P, 1999.

Guild, Jennifer. Scripting Quality of Security Service (QoSS) Safeguard Measures for the Suggested INFOCON System. Master's Thesis. Naval Postgraduate School, 2004.

Harris, Shon. CISSP All-in-One Exam Guide. 2nd ed. McGraw-Hill Osborne Media, 2003.

Herman, Debra S. A Practical Guide to Security Engineering and Information Assurance. Boca Raton: CRC P LLC, 2002.

Hesse, Rick. "Triangle Distribution: Mathematica Link for Excel." Editorial. Decision Line May 2000.

Horizontal Integration: Broader Access Models for Realizing Information Dominance. MITRE Corporation. McLean, Virginia: JASON Program Office, 2004.

Martin, Jean-Christophe. Policy-Based Networks. Sun Microsystems, Inc. Palo Alto: Sun BluePrints™ OnLine, 1999. 16 Nov. 2006 <http://www.sun.com/blueprints>.

McGraw, Robert W. Risk-Adaptable Access Control (RAdAC) an Access Control Model to Support the Goals of Information Superiority. National Security Agency. 2006.

McGraw, Robert W. “Securing Content in the Department of Defense’s Global Information Grid.” Secure Knowledge Management Workshop. State University of New York, Buffalo. 23 Sept. 2004.

Montry, Kenneth. IA Risk Assessment Process. IEEE Workshop on Information Assurance and Security, 16 June 2005, United States Military Academy, West Point, NY.

Morgan, Millett G., and Max Henrion. Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis. Cambridge: Cambridge UP, 1990.

Mun, Johnathan. Applied Risk Analysis. Hoboken: John Wiley & Sons, Inc., 2004.

Mun, Johnathan. Modeling Risk. Hoboken: John Wiley & Sons, Inc., 2006.

Peltier, Thomas R. Information Security Risk Analysis. 2nd ed. Boca Raton: CRC P LLC, 2005.

Pfleeger, Charles P., and Shari L. Pfleeger. Security in Computing. 3rd ed. Upper Saddle River: Pearson Education, Inc., 2003.

Sheldon, Tom. Encyclopedia of Networking & Telecommunications. McGraw-Hill, 2001.

Smith, Rick. “Introduction to Multilevel Security.” University of St. Thomas. 31 Oct. 2005. Quantitative Methods and Computer Science, University of St. Thomas in Minnesota. 10 Nov. 2006 <http://www.cs.stthomas.edu/faculty/resmith/r/mls/index.html>.

United States. Chief of Naval Operations. Department of Defense. Information Assurance (IA) Publication 5239-16 Risk Assessment Guidebook. 2003.

United States. Department of Defense. Defense Acquisition Guidebook. 2006.

United States. Department of Defense. Directive 8100.1. 2002.

United States. Department of Defense. Transformation Planning Guidance. 2003.

United States. Joint Chiefs of Staff. Department of Defense. Net-Centric Operational Environment Joint Integrating Concept. 2005.

United States. United States Strategic Command. Department of Defense. Joint Concept of Operations for Global Information Grid NetOps. 2005.

Vose, David. Risk Analysis. 2nd ed. New York: John Wiley and Sons, Inc., 2000.

Yavatkar, R, D Pendarakis, and R Guerin. RFC 2753: A Framework for Policy-Based Admission Control. Internet Engineering Task Force. The Internet Society, 2000.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dr. George Dinolt
   Naval Postgraduate School
   Monterey, California

4. Lt Col Karl Pfeiffer
   Naval Postgraduate School
   Monterey, California

5. Dr. Dan Boger
   Naval Postgraduate School
   Monterey, California

6. Prof. Simson Garfinkel
   Naval Postgraduate School
   Monterey, California

7. Dr. Steven Borbash
   National Security Agency
   Ft. Meade, Maryland

8. Mr. Lewis Weinstein
   National Security Agency
   Ft. Meade, Maryland

9. Mr. Steven LaFountain
   National Security Agency
   Ft. Meade, Maryland